UNIVERSITÀ DI PISA

Dipartimento di Giurisprudenza

LAUREA MAGISTRALE IN GIURISPRUDENZA

La *Digital Evidence:* il difficile contemperamento tra esigenze investigative e garanzie del processo penale

Candidata:
Federica Lucà

Relatore:
Prof.ssa Benedetta Galgani

Anno Accademico 2013 - 2014

Ai miei genitori

INDICE

II.2.1 Il labile confine tra ispezione e perquisizione in ambito informatico.

II.2.2 La *preview* dei reperti.

II.2.3 La perquisizione digitale: profili di incostituzionalità.

II.3 Il Sequestro probatorio informatico.

II.3.1 Il sequestro di corrispondenza.

II.3.2 Il sequestro di dati informatici.

II.3.3 La tutela dei supporti posti sotto sequestro.

II.4 Le intercettazioni telematiche.

II.4.1 La conformità al dettato costituzionale.

II.4.2 L'ambito oggettivo di applicazione.

II.4.3 I presupposti procedurali: gravi indizi di reato e assoluta indispensabilità

II.4.4 Intercettazioni mediante impianti appartenenti a privati.

II.4.5L'analisi dei dati oggetto di intercettazione.

II.5 L'alibi informatico: definizione e consistenza

II.5.1 Il ruolo dell'alibi informatico.

II.5.2 Il "falso alibi".

II.6 Le *"Malpractices"* nella *digital forensics*: giurisprudenza a confronto.

II.6.1 Gli *standard* di tutela della prova digitale e il caso *Vierika.*

II.6.2 Il caso di Garlasco.

Capitolo III
LA NORMATIVA SULLA *DATA RETENTION*: *PRIVACY* E SICUREZZA INFORMATICA

CAPITOLO I
CRIMINE INFORMATICO E RICERCA DELLA PROVA: LE INVESTIGAZIONI INFORMATICHE

I.1 *Il Cybercrime nel diritto penale italiano*

Un primo tentativo del legislatore italiano teso a contrastare la cosiddetta "criminalità informatica" risale al 1993, allorquando venne emanata la legge 23 dicembre 1993 n. 547[1].

L'introduzione di tale normativa si rese necessaria, giacché il tentativo di applicare le fattispecie delittuose presenti nel codice penale, ai comportamenti criminosi commessi a mezzo del *personal computer* e della rete informatica, pareva operazione ermeneutica di dubbia fattibilità.

Rilievi critici fondamentali, erano quelli relativi alla possibile violazione dei principi di tassatività e legalità penali.

L'inadeguatezza degli strumenti classici del diritto penale, rendeva dunque pressochè privi di punizione i comportamenti che si sostanziassero in un *cybercrime*: proprio come risposta a tale lacuna si deve leggere l'intervento normativo del 1993, recante il titolo "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica".

1 G.U. Del 30 dicembre 1993, n.305

Il suddetto intervento ha disciplinato i reati informatici "classici", vale a dire quelli commessi su beni informatici (computer, sistemi informatici o telematici,dati informatici ecc).[2]

La categoria dei *cybercrimes*, infatti, è aperta, ed include, accanto a reati informatici "classici", che prevedono specificamente tra i loro elementi costitutivi espressi riferimenti a mezzi ed oggetti informatici, "qualsiasi altra incriminazione, offensiva di beni giuridici comuni, se applicabile, anche in via interpretativa a comportamenti e fatti posti in essere avvalendosi (anche) di *Internet* e della tecnologia delle telecomunicazioni. Situazione che può frequentemente verificarsi nei reati di evento o, comunque, formulati in tutto od in parte a forma libera"[3].

Si tratta, in relazione a tali ultime fattispecie, di casi in cui il reato è commesso non sulle nuove tecnologie bensì per mezzo delle stesse, di illeciti penali realizzabili anche in altri ambiti ma commessi nel caso di specie tramite lo strumento *Internet*.

I *cybercrimes* ricomprendono fattispecie di reati informatici e telematici estremamente diversi tra loro (dalla pedofilia telematica al danneggiamento di sistema informatico) che offendono interessi del tutto differenti, riconducibili tuttavia a due macrocategorie.

La prima è rappresentata da alcuni beni giuridici tradizionali

---

2C.SANTORIELLO, *La legge di ratifica della Convenzione di Budapest ed il nuovo diritto penale dell'informatica,* dal testo *I Reati informatici. Nuova disciplina e tecniche processuali d'accertamento,* (a cura di) G.Amato, V.S.Destito, C.Santoriello, Cedam, 2010, p. 1.

3L.PICOTTI, *Sistematica dei reati informatici, tecniche di tutela e beni giuridici tutelati,* dal testo *Il diritto penale dell'informatica nell'epoca di Internet,* Padova, 2004, p.21 ss.

che devono essere protetti contro nuove modalità di aggressione (come avviene per la tutela dei minori o del patrimonio), nonché da una serie di beni giuridici analoghi a quelli tradizionali radicati su nuovi "oggetti passivi" della condotta (ovvero il prodotto della tecnologia informatica o telematica su cui cade la condotta tipica, con conseguente determinazione di una speciale configurazione o dimensione del bene giudico protetto: ad esempio, fede pubblica nei documenti informatici, diritto d'autore, protezione penale della *privacy* e della circolazione dei dati personali).

Alla seconda categoria, appartengono invece, i beni giuridici nuovi nati dall'informatica e dalla telematica, raggruppabili a loro volta in due sottospecie: l'integrità e sicurezza informatica e la riservatezza informatica.

Ciò che sembra invece accomunare e poter identificare univocamente i *cybercrimes,* è la loro interconnessione con le nuove tecnologie, ovvero con l'informatica ed i suoi prodotti e con la telematica.

Tale interconnessione può concernere i mezzi e le modalità di realizzazione della condotta, la natura informatica dell'oggetto materiale della fattispecie o ancora il bene giuridico di nuova emersione legato ai prodotti della tecnologia digitale tutelato dalla norma penale; questi diversi profili, peraltro, incidono sempre sulla struttura del fatto tipico e sulla *ratio* dell'incriminazione, che finisce solo in parte per coincidere con l'oggettività giuridica tradizionale eventualmente corrispondente.

I.1.2 ***La Convenzione di Budapest***

Trascorsi meno di dieci anni dalla legge cui si è fatto cenno, è emerso in ambito internazionale un nuovo e più intenso bisogno di repressione delle condotte criminose realizzate a mezzo degli strumenti informatici.

La consapevolezza della valenza e della rilevanza internazionale del fenomeno del *cybercrime,* ha quindi trovato pieno riconoscimento con l'approvazione da parte del Consiglio d' Europa in data 23 novembre 2001 della cosiddetta "Convenzione di Budapest", che rappresenta il primo accordo internazionale riguardante i reati commessi tramite *internet* o altre reti elettroniche.

Con la Convenzione di Budapest il Consiglio d'Europa – consapevole della rilevanza transnazionale delle condotte di criminalità informatica – ha cercato di dettare agli Stati membri alcuni principi cui ispirarsi nella regolamentazione del fenomeno del *cybercrime.*

La finalità era quella di delineare un sistema in cui le problematiche di rilevanza penalistica insorte a seguito dello sviluppo di *internet* e delle connessioni telematiche, fossero regolamentate in maniera tendenzialmente uniforme nei vari ordinamenti nazionali.

Com'è stato detto, infatti, *"l'obiettivo primario della Convenzione sulla criminalità informatica, risiede nell'esigenza di introdurre...un minimum target di tutela dei beni giuridici offesi dai cybercrimes ed un livello minimo essenziale comune di strategie di contrasto a tali illeciti,*

soprattutto in ragione della loro natura tendenzialmente trans-nazionale, che comporta chiaramente la necessità dell'armonizzazione della relativa normativa di contrasto nell'ambito dei vari ordinamenti"[4].

A tale scopo, il Consiglio d'Europa ha ritenuto che l'integrazione dei diversi ordinamenti europei richiedesse necessariamente l'osservanza di alcune condizioni e la presenza di diversi presupposti concettuali.

In primo luogo, la Convenzione contiene una serie di modelli di incriminazione uniformi, diretti a realizzare un livello di tutela penale omogeneo per beni giuridici aggrediti dalle condotte di criminalità informatica.

Ciò è stato dettato sia allo scopo di impedire che in sede di cooperazione internazionale possa venir meno il requisito della "doppia incriminazione", sia per consentire l'applicazione dei principi dettati dalla Convenzione non solo ai *cybercrimes,* ma anche a tutte le fattispecie commesse mediante un sistema informatico o per le quali vi siano prove in formato elettronico.

In secondo luogo, nell'atto pattizio viene individuata e suggerita la definizione di un adeguato sistema di collaborazione fra gli organismi nazionali e sopranazionali.

L'Accordo internazionale, contiene altresì la descrizione delle condotte ritenute penalmente rilevanti ossia: le fattispecie di accesso abusivo, di intercettazione illegale, di attentato all'integrità dei dati e dei sistemi, di abuso di apparecchiature, di falsificazione informatica, di pornografia

4 C.SANTORIELLO, *I reati informatici. Nuova disciplina e tecniche processuali d'accertamento,* (a cura di) G.Amato, V.S.Destito,G.Dezzani, C.Santoriello, Cedam, 2010, p. 3 ss.

infantile e di violazione della proprietà intellettuale.

Il medesimo Accordo, stabilisce che tali condotte criminose siano sanzionate con "pene effettive, proporzionate e dissuasive, ricomprendenti anche la privazione della libertà personale"[5].

Ulteriori indicazioni sono fornite in relazione alle indagini che sono necessarie per un'effettiva repressione dei *cybercrimes*, richiedendo che gli Stati membri – una volta acquisita la prova della commissione degli illeciti predetti – provvedano ad assumere misure idonee a garantire la conservazione dei dati informatici facilmente soggetti a modificazione ed al mantenimento dell'integrità delle informazioni, per il tempo necessario all'individuazione dei colpevoli ed all'accertamento processuale della loro responsabilità.

La Convenzione, inoltre, richiede che vengano introdotte regole uniformi in tema di perquisizione, sequestro ed accesso a sistemi, dati e supporti informatici, nonché per la raccolta e registrazione in tempo reale dei dati relativi al traffico, intercettazione e registrazione di comunicazioni telematiche.[6]

Onde rendere più celere lo svolgimento di tali indagini, in ambito di collaborazione tra i vari Stati, la richiesta di mutua assistenza può essere formulata, in casi di urgenza, anche mediante mezzi di comunicazione come *fax* e posta elettronica, purché siano assicurate appropriate garanzie di sicurezza, cui segua poi la conferma ufficiale se lo Stato

5 Art. 13 della Convenzione.

6 Art. 19,20 e 21 della Convenzione.

richiesto lo ritenga necessario.[7]

I.2 *La legge di ratifica della Convenzione di Budapest*

Con la L.18 marzo 2008 n. 48 il legislatore italiano ha ratificato e dato esecuzione alla Convenzione di Budapest sulla criminalità informatica.

Si tratta di una legge complessa, che in ossequio alla ripartizione contenuta nel provvedimento ratificato, prevede disposizioni di diritto penale sostanziale e processuale.

L'ampio decorso del tempo che è intercorso dalla firma della Convenzione suddetta, avrebbe in verità, consentito al legislatore italiano di dare altresì attuazione alla Decisione quadro 2005/222/GAI del Consiglio UE del 24 febbraio 2005, avente ad oggetto gli attacchi contro i mezzi di informazione, largamente ispirata alla Convenzione stessa[8].

Il legislatore, tuttavia, non ha colto l'occasione rappresentata dalla ratifica della Convenzione del 2001 per adeguare l'ordinamento interno anche alla decisione del 2005.

La conseguenza di questa colpevole mancanza, è che l'efficacia internazionale delle disposizioni contenute nella legge è inevitabilmente dimidiata dal mancato riferimento al fondamentale atto adottato successivamente dall' Unione Europea.

Reso conto di questa carenza, si deve rilevare che un intervento di razionalizzazione della materia era largamente

---

7 Art. 23 della Convenzione.

8 G.MORGANTE, L.18/03/2008 n.48 – *Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno (G.U* 4.4.2008 n.80), in *Legislazione Penale 2008,* p. 251ss.

atteso, anche in considerazione della limitatezza e delle non poche questioni interpretative sollevate dalla l. 547/1993 avente ad oggetto modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale.

Senonchè, pur essendo idealmente preceduto da un provvedimento avente ad oggetto la medesima materia, sul versante del diritto penale sostanziale il legislatore del 2008 ha preferito non seguire la consueta tecnica della novellazione delle disposizioni già esistenti, procedendo invece all'introduzione di nuove fattispecie incriminatrici.

Diversamente, si è scelto invece di procedere con riferimento all'aspetto processuale della riforma.

Sul piano della competenza, è stata stabilita la competenza per materia dell'ufficio del Pubblico Ministero presso il tribunale del capoluogo del distretto nel cui ambito ha sede il Giudice competente (art. 11 l . 48/2008, che aggiunge il comma 3 – *bis* all'art. 51 c.p.p.).

Un tema cruciale nell'ambito della criminalità con mezzi informatici su cui si concentra essenzialmente la legge in esame è quello delle "prove".

È proprio dalla parte processualistica della riforma che traspare il rilievo della materia in esame.

È significativo sottolineare che l'aumento esponenziale dell'uso delle tecnologie informatiche comporta non soltanto il progressivo incremento della criminalità informatica propriamente detta, ma anche il ricorso a mezzi informatici nell'ambito di altre forme di criminalità (es. la criminalità organizzata).

Le disposizioni processuali sulla ricerca e la conservazione

delle *digital evidences* sono infatti suscettibili di trovare applicazione in un ambito molto più ampio del ristretto sistema di quelli che tradizionalmente sono nominati reati informatici.

In maniera più specifica la legge in analisi ha modificato il codice di procedura penale nella sezione relativa ai mezzi di ricerca della prova ed alle indagini di polizia giudiziaria, attraverso l'indicazione di specifiche modalità di esecuzione di ispezioni, perquisizioni e sequestri, con la prescrizione di apposite regole di conservazione, di intangibilità degli originali dati informatici e di conformità delle copie.[9]

Si deve però sottolineare, che gli innesti al codice di rito apportati per adeguare la sua architettura sistematica all'impostazione teorica sottesa alla convenzione, non sono il frutto di una operazione forzata, volta appunto a rispettare pedissequamente gli impegni internazionali assunti.

Potremmo dire, piuttosto, che l'obbligo pattizio ha fornito lo spunto per mettere mano in maniera più celere ad una azione già meditata *motu proprio* da tempo, e fortemente patrocinata da gran parte della dottrina.

Gran parte degli studiosi e degli operatori del diritto processuale penale, infatti, da tempo denunciavano: da un lato le difficoltà ermeneutiche insite nell'utilizzo dei tradizionali istituti processuali per l'apprensione del dato digitale e, dall'altro, segnalavano il rischio che in mancanza di un intervento legislativo, lentamente si potesse scivolare verso un fenomeno che potremmo definire di "deriva

9 C.SANTORIELLO, *La legge di ratifica della Convenzione di Budapest ed il nuovo diritto penale dell'informatica,* dal testo *I Reati informatici. Nuova disciplina e tecniche processuali d'accertamento,* (a cura di) G.Amato, V.S.Destito, C.Santoriello, Cedam 2010.

tecnicistica".

Secondo un certo orientamento, infatti, si sarebbe dovuta ipotizzare "un'autonomia sistematica delle operazioni di *computer forensics,* ritenute in virtù della loro peculiarità un settore disancorato dal resto del *corpus* normativo"[10].

La verità è che, malgrado i redattori della l. 48/2008 abbiano certamente tenuto conto degli esiti di tale dibattito, il risultato finale non può dirsi del tutto soddisfacente, anche in ragione di un'affrettata approvazione determinata dalla intervenuta caduta dell'esecutivo e dalla repentina chiusura dell'attività parlamentare.

Quest'ultima constatazione è da riferirsi altresì alle questioni di diritto sostanziale della materia.

Sotto il profilo del diritto penale sostanziale, infatti, si è posto come problema fondamentale la dubbia scelta del legislatore italiano di affrontare situazioni nuove con strumenti antichi, e spesso del tutto inadeguati, dove le fattispecie di nuovo conio presentano non pochi problemi pratico-applicativi, caratterizzati tra l'altro da una marcata eterogeneità rispetto ai modelli d'origine[11].

In merito al profilo processual-penalistico, non può che essere definita parzialmente deludente, la scelta di ridurre al minimo gli interventi e di procrastinare le necessarie prese di posizione rispetto alle numerose controversie ermeneutiche emerse in questi anni sul piano della prassi giudiziale[12].

---

10 L.LUPARIA, *I profili processuali,* in *Dir. pen. proc.,* 2008*,* p. 717

11G.MORGANTE, L.18/03/2008 n.48 – *Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno (G.U* 4.4.2008 n.80), in *Legislazione Penale 2008,* p. 253.

12 L.LUPARIA, *I profili processuali,* in *Dir. pen. proc.,* 2008*,* p. 718.

Argomenti quali la captazione delle comunicazioni vocali effettuate con sistemi *voice – overIP*[13], le intercettazioni parametriche,[14] l'apprensione in tempo reale della posta elettronica, le attività di agente "provocatore informatico" condotte dalla Polizia Giudiziaria, i limiti al sequestro del *computer* dell'indagato o del soggetto terzo, solo per citarne alcuni, non hanno trovato spazio in questa "mini" riforma dell'ordito codicistico, circostanza quest'ultima che lascia presagire la necessità di ulteriori correttivi in un futuro prossimo.

I.3 La *Computer Forensics* e le *Best practices*

I.3.1 La *Computer Forensics*

La "*Computer Forensics*" è una disciplina nata negli Stati Uniti d'America nella seconda metà degli anni Ottanta del secolo scorso, in occasione dello sviluppo da parte dell'FBI e di altre agenzie investigative americane di programmi e degli strumenti, adoperati per recuperare gli elementi di prova digitali all'interno di un *computer*[15].

Come si è già avuto modo di far cenno precedentemente, con lo sviluppo della tecnologia informatica, si è avuto un incremento di azioni e di condotte criminali basate

---

13 Essendo venuta meno l'iniziale netta distinzione tra sistemi telefonici e sistemi informatico-telematici, si sta facendo strada la proposta di ricomprendere le telefonate effettuate con l'oramai diffusissimo vettore *Skype*, all'interno delle più larghe maglie dell'art 266 c.p.p.

14 Si tratta di captazioni che agiscono per parola chiave e su larga scala. Gli organi investigativi monitorano in sostanza tutto il traffico nazionale o regionale di un determinato *provider* filtrandolo mediante uno specifico parametro (una parola, un indirizzo *web*, ecc.)

15 S.ATERNO, *Acquisizione e analisi della prova informatica*, in *Dir. Pen. Proc.*, 2008, cit., p.61

sull'utilizzo di sofisticati strumenti telematici e di telecomunicazione, che determinano la presenza sulla *scena criminis* di numerosi elementi di prova digitale.
L'ambito di applicazione di questa tecnica dipende in parte dall'oggetto delle sue attenzioni.
In base ad esso si distinguono infatti:
- la *computer forensics in senso stretto*, con riferimento all'analisi dei dispositivi e supporti fisici e statici
- la *network forensics*, che ha come oggetto l'analisi forense di server e di reti
- la *mobile forensics*, che analizza i dispositivi cellulari e mobili
- la *PDA forensics,* che infine esamina con modalità forensi i telefoni palmari di ultima generazione.

Lo scopo della *Computer forensics* è conservare, identificare, acquisire, documentare e interpretare dati rilevanti per il diritto, senza alterare o modificare i dati medesimi o il *file* syste*m* del *computer*.
Detti dati, infatti, potrebbero essere utili al fine di reperire "fonti di prova", ovverosia a permettere la ricostruzione della dinamica attraverso la quale è stato perpetrato l'illecito penale.
Per questo motivo, è opportuno comprendere il significato delle evidenze digitali e la loro portata, nel corso dell'esecuzione di un'attività di *computer forensics.*
Le evidenze digitali, sono quelle fonti di prova memorizzate in strumenti informatici, come le postazioni di lavoro degli utenti, i *server* aziendali o altri sistemi informatici.

Questo tipo di evidenze sono caratterizzate da una "carenza di fisicità" che porta ad una maggiore facilità di modifica accidentale durante la fase di acquisizione delle stesse.
Si consideri ad esempio l'atto di aprire un documento di testo, che potrebbe essere utili alle indagini.
Tale apertura, può essere sufficiente per modificarne alcune caratteristiche. Affinché il dato sia mantenuto intatto, è quindi, necessario, agire con la massima attenzione e attraverso l'ausilio di strumenti appositi.
Tale obiettivo è perseguito mediante l'utilizzo di *Tools Forensics,* cioè programmi applicativi che consentono l'acquisizione, la custodia e l'analisi dei elementi di prova informatici ed, inoltre, mediante la predisposizione di modalità operative per gli operatori del diritto dette "*Best practices"*[16].

I.3.2 **Le *Best practices***

Una particolare attenzione, va dedicata alle *best practices*, le quali, come si è fatto cenno, consistono nelle modalità operative dettate per gli operatori del settore.
Esse sono elaborate dai singoli organi di investigazione scientifico-tecnologica, secondo esperienze pratiche ed elaborazioni dottrinali: tra le più importanti, quelle di Eoghan Casey[17], e, a livello italiano, quelle di Cesare Maioli[18]; vi

16 F.NOVARIO, *Le prove informatiche,* dal testo *La Prova Penale*, a cura di P.Ferrua, E.Marzaduri, G.Spangher, cit., p.124ss.
17 E.CASEY, è un esperto riconosciuto a livello internazionale in materia di indagini sulla violazione dei dati e sicurezza informatica forense, il suo lavoro più importante si ricollega alla scrittura del libro *Digital evidence and computer crime.*
18 C.MAIOLI, professore ordinario di informatica giuridica presso la

sono altresì *best practices* di organizzazioni investigative internazionali, tra cui l' *United State Secret Service,* l'*International association of Chiefs of Police,* il *National Institute of Justice* e l'*Association of Chief Police Officers.*

Ciò premesso, è possibile elaborare un modello generale di *best practices* suddiviso in 3 fasi: la fase degli *Adempimenti preliminari*, la fase di *Ricerca di materiali rilevanti*, infine, la fase dell' *Analisi e documentazione dello stato dei luoghi.*

Gli Adempimenti preliminari consistono nella scelta dell'equipaggiamento tecnico idoneo al caso concreto e nella messa in sicurezza della *scena criminis* materiale.

La fase di Ricerca di materiali rilevanti si apre dopo aver compiuto l'isolamento del luogo e deve seguire un rigore logico, consistente:

- nella ricerca dell'hardware, del software e della documentazione ad essi relativa
- nella ricerca di informazioni relative a password o account
- nel vaglio di stampe e scarti presenti in *loco*
- nella ricerca, da ultimo, di altri materiali rilevanti per il caso concreto.

La fase di Analisi e documentazione dello stato dei luoghi, infine, si occupa:

- di verificare lo stato di attività delle connessioni di rete e dei computer, le fotografie dei luoghi e degli schermi dei monitor
- di rilevare le impronte digitali dalle periferiche
- di interrompere i programmi lesivi dell'integrità dei dati

---

facoltà di giurisprudenza di Bologna, autore di 16 monografie ed oltre 200 articoli scientifici e tecnici, esperto in materia di *computer science.*

- di salvare le operazioni informatiche in corso
- di preservare il contenuto della memoria RAM
- di valutare l'opportunità di procedere al sequestro del computer oppure calcolare l'algoritmo di Hash[19] e successiva copia dei dati originali
- di etichettare e classificare i reperti materiali rinvenuti[20].

Corrette modalità di conservazione, procedure di duplicazione efficaci, garanzie di non alterabilità ed *extrema ratio* del sequestro di servizi sono, in conclusione, i quattro principi della *Computer forensics* introdotti dalla l. 48/2008 nel nostro ordinamento.

I.4 Il dato informatico e la sua efficacia probatoria: l'individuazione, l'acquisizione, l'analisi e la presentazione.

Si può considerare *digital evidence* ogni informazione probatoria la cui rilevanza processuale dipende dal contenuto del dato o, dalla particolare allocazione su di una determinata periferica, oppure dal fatto di essere stato trasmesso secondo modalità informatiche o telematiche[21].
Si deve tener conto di un fondamentale aspetto del dato informatico, ossia che esso è per sua natura insuscettibile di

19 *L'algoritmo di Hash* è il valore ottenuto come risultato matematico. Viene utilizzato in informatica forense per garantire che un dato non abbia subito alterazioni.
20 F.NOVARIO, *Le prove informatiche,* dal testo *La Prova Penale*, a cura di P.Ferrua, E.Marzaduri, G.Spangher, p. 126.
21 L.MARAFIOTI, *Digital evidence e processo penale,* in *Cass. pen.,* 2011, p. 4509 ss.

percezione sensoriale, in quanto ontologicamente caratterizzato da immaterialità e volatilità.

La composizione del dato digitale, è data da una sequenza di *bit,* dove *bit* sta per *binary digit* ed esprime l'alternativa tra 0 e 1, come unità minima di informazione logicamente possibile.

A differenza del documento tradizionale di tipo analogico, che è il mezzo utilizzato per incorporare la rappresentazione del fatto in una base materiale, il documento informatico prescinde dal tipo di supporto fisico su cui è fissato il dato ed in ogni momento può essere prelevato e trasferito su altro supporto idoneo a recepirlo[22].

Sono 4 le fasi che caratterizzano il trattamento del reperto informatico: l'individuazione, l'acquisizione, l'analisi e la presentazione.

L'individuazione del reperto informatico non è un'operazione semplice, in quanto se il reperto non viene prontamente individuato, si espone per un tempo maggiore al rischio di inquinamento, se non alla sua distruzione vera e propria.

Ulteriore aspetto da considerare in questa fase è la corretta conservazione ed imballaggio del supporto su cui sono registrati i reperti. In base alla tipologia del reperto andranno accuratamente scelte gli opportuni contenitori e anche le modalità di conservazione.

La fase acquisitiva del dato informatico è la più delicata e complessa in assoluto. Essa consiste sostanzialmente in un'operazione di estrapolazione e riproduzione su idoneo supporto del dato digitale oggetto di indagine.

---

22 S.VENTURINI, *Sequestro probatorio e fornitori di servizi telematici,* dal testo *Internet provider* di L.Lùparia, Giffrè 2009.

Tutto deve svolgersi nella piena garanzia di integrità e non alterabilità delle tracce e nella prospettiva di una possibile successiva ripetibilità dell'operazione, al fine di consentire una eventuale conseguente verifica della genuinità del dato informatico.

Tale fase viene effettuata attraverso la c.d *bit stream image ,* ovverosia, la realizzazione di una "immagine" *bit a bit* del contenuto del supporto posto sotto sequestro, che consente di operare l'analisi forense su un *hard disk*[23] identico all'originale sia sotto il profilo logico che fisico.

Questa analisi deve quindi essere condotta anche su tutte quelle parti "vuote" o presumibilmente tali, che potrebbero assumere grande rilevanza ai fini delle indagini, in quanto possono nascondere *file* o frammenti di *file* (c.d. *Slack)* cancellati[24].

È possibile osservare l'attitudine probatoria dei *file* suddividendoli in due categorie: le "evidenze informatiche" -file testuali, multimediali o di archivio- la cui sola presenza può far riscontrare l'evento e la condotta di un illecito ed i "programmi", cioè *file* che necessitano di un'analisi per divenire evidenti.

Nel caso delle evidenze informatiche, le proprietà dei *file* - data, ora e utente di creazione, cancellazione e modificazione - possono divenire informazioni utili per una corretta ricostruzione cronologica dei fatti e una corretta attribuzione di responsabilità dell'utente.

---

23 L'hard disk è il cuore del sistema, è il luogo in cui vengono registrati e in parte conservati i dati, in *Diritto Penale e Processo,* 2008, cit.p.63.

24*Slack:* è una porzione di ciò che rimane di un *file*, quando viene cancellato superficialmente e sopra il quale in parte il sistema informatico stesso riscrive.

Nel caso invece dei *file* di programma, che possono essere applicativi o di sistema, un particolare tipo risulta rilevante: i *log*.

Questi *file* sono generati in automatico da programmi attivi nel sistema *software* e presenti nelle memorie di massa, sono di tipo testuale e contengono la registrazione di tutte le informazioni sul programma che li ha generati e sulle sue attività. I *file* di *log* sono facilmente manipolabili e sovrascritti dal sistema in breve tempo, così da renderne utile l'analisi solo a breve termine dalla commissione dell'illecito[25].

In relazione alla delicatezza di questa fase, tutte le operazioni di individuazione del reperto informatico dovrebbero essere accuratamente documentate, possibilmente utilizzando dispositivi che registrino automaticamente quanto eseguito.

La fase dell'Analisi del reperto informatico avviene invece attraverso strumenti altamente sofisticati, in grado di analizzare qualunque *file*, anche quelli cancellati o parti di file residuati nella memoria di un *hard disk*[26]ed individuare la *timeline,* ossia il momento in cui è stata eseguita l'ultima modifica del *file.*

Bisogna sempre tenere presente che un'indagine di informatica forense non avviene mai sul sistema informatico originale, bensì su una *copia* dei supporti sui quali lavorare in un secondo momento.

Le operazioni da compiere possono essere di varia natura e

25F.NOVARIO, *La Prova Penale*, a cura di P.Ferrua, E.Marzaduri, G.Spangher, cit.p. 127

26S.ATERNO, *Acquisizione e analisi della prova informatica*, in *Dir. Pen. Proc.*, 2008, cit., p.64

dipendono strettamente dalla tipologia del reato oggetto di indagine.

Le principali attività di analisi effettuabili su un dato digitale sono le seguenti:

1. *Text searching:* consiste nel condurre ricerche di tipo testuale all'interno dei *file* o delle *directory* e si estende a tutte le strutture del *file system*. L'analisi del contenuto di file con applicazione ignota viene effettuata con l'impiego di visualizzazioni forensi in grado di interpretare numerosi formati.[27]
2. *Image searching:* consiste nella ricerca delle immagini digitali su file di vario formato, inclusi i fotogrammi di *file* video e riveste grande importanza nei casi di pedopornografia e di violazione del diritto d'autore.
3. *Data recovery e idenfication:* questa fase dell'analisi è di grande utilità per la quantità di informazioni che può fornire all'operatore: è costituita appunto dalla *data recovery* (che consiste nel procedimento per recuperare dati presenti, cancellati, o danneggiati da memorie di massa), dalla *data discovery* (che consiste nel procedimento per scoprire dati nascosti da una memoria o da *file* cifrati o protetti in altro modo) e dalla *data carving* (che consiste nel tentativo di ricostruire un *file* danneggiato attraverso il recupero di porzioni di *file*.
4. *Metadata recovery e identification*: i metadati sono

27 G.VACIAGO, *Digital evidence. I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato,* cit.p.98 ss.

dei dati che rivestono particolare importanza e comprendono informazioni di sistema o applicazioni a corredo della struttura di *file system, file,* cartelle, partizioni.

Il recupero e l'identificazione dei dati (es. date e orari, attributi di file) sono rilevanti al fine di determinare la *timeline* di accesso e di modifica di un *file*.

Il volume dei dati contenuti all'interno di un supporto da analizzare e la rapidità con cui si evolvono gli strumenti di analisi per le indagini digitali, impediscono di prevedere una rigida procedura da seguire: in questa fase infatti è fondamentale la capacità investigativa e l'esperienza del *digital forenser.*

L' ultima fase è quella della Presentazione delle conclusioni che viene effettuata dal consulente tecnico a seguito della propria attività d'accertamento: qualora la presentazione dei risultati non consegua il risultato di trasmettere a tutti gli interessati i fatti accertati con la chiarezza necessaria, l'intero iter rischierà di essere vanificato[28] .

La relazione tecnica potrà essere redatta in fase di accertamento tecnico preventivo, incidente probatorio e perizia.

Negli ultimi due casi viene instaurato un vero e proprio contraddittorio davanti al Giudice, nel primo invece, il consulente lavorerà a stretto contatto con la Procura e la Polizia Giudiziaria, salvo che egli non abbia ricevuto l'incarico da parte di un avvocato di controllare il loro

28 S.Aterno, *Acquisizione e analisi della prova informatica*, in *Dir. Pen. Proc.*, 2008, cit., p.64.

operato o di effettuare delle autonome indagini difensive.

Indipendentemente dalla fase in cui viene richiesta, la relazione tecnica deve necessariamente contenere una completa ed esaustiva descrizione dei sistemi informatici analizzati, un elenco degli strumenti (*tools*) utilizzati e un dettagliato resoconto dei risultati raggiunti.

Quasi tutti i *software* di analisi forense hanno infatti dei *tools,* che consentono di registrare tutte le attività compiute dall'esperto e successivamente di inserire le prove digitali direttamente nel *report*, tuttavia, poiché l'elenco delle operazioni compiute è scritto in inglese, può risultare più complesso l'utilizzo di questi strumenti da parte della P.G. o del Consulente tecnico.

La sfida più delicata è quella di presentare il caso in modo che non vi possano essere eventuali contestazioni: da un lato infatti, la *presentazione* deve essere immediata e di facile comprensione, ma dall'altro non deve dare adito a contestazioni sul metodo eseguito.

Non bisogna dimenticare inoltre che la relazione tecnica viene spesso redatta con largo anticipo rispetto alla fase in cui verrà effettivamente analizzata, è necessario quindi essere il più dettagliati e conformi possibili alle *best practices* in materia[29].

29 G.VACIAGO, *Digital evidence. I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato.* cit.p.100

I.4 Gli accertamenti tecnici: definizione terminologica

Nel codice di procedura penale, numerosi sono i richiami terminologici ai "rilievi" ed agli "accertamenti", nomenclature che sovente vengono utilizzate indiscriminatamente e senza distinzione alcuna.

Così, nell'art. 349, 2° co., c.p.p. il legislatore, a proposito dell'attività esperibile dalla Polizia Giudiziaria ai fini dell'identificazione della persona, nei cui confronti vengono eseguite le indagini e di altre persone, richiama eventuali rilievi dattiloscopici, fotografici e antropometrici, nonché altri accertamenti.

A sua volta l'art. 358 c.p.p., fa esclusivo riferimento agli accertamenti che, *ex lege*, il Pubblico Ministero deve svolgere nei confronti della persona indagata.

Ancora, l'art. 359 c.p.p., nell'individuare l'attività del Pubblico Ministero, fa cenno ad accertamenti e rilievi segnaletici, descrittivi o fotografici.

Questa mancata uniformità terminologica, si denota con più chiarezza, se si prosegue nella lettura dell'art. 360 c.p.p., che rinvia agli accertamenti contenuti nell'art. 359 c.p.p., senza però citare i rilievi cui fa riferimento quest'ultimo articolo.

Al fine di ripristinare, quindi, la chiarezza richiesta dal diritto, sarà essenziale palesare il significato di questi termini.

Con riferimento ai "rilievi", si deve generalmente intendere, un'attività di individuazione e rilevazione di dati materiali; mentre per "accertamenti" si deve intendere un'attività di

studio, di analisi e di giudizio di quegli stessi dati[30].

Ciò premesso, sarà possibile definire "rilievo", ad esempio, l'attività di raccolta dattiloscopica, mentre sarà "accertamento", lo studio di tali impronte e il confronto con quelle presenti nel "*database"* delle persone segnalate.

Da questa distinzione, potrebbe dunque concludersi, con tutte le cautele del caso, dato il silenzio del legislatore in merito, che i rilievi siano prodromici agli accertamenti e, che esista una sorta di rapporto di *species at genus* degli uni rispetto agli altri[31].

A contestazione di chi[32] attribuiva ai rilievi il ruolo di "forme speciali di accertamento" e, allo stesso tempo, qualificava entrambi gli strumenti come "il punto di emergenza o la risultante di mezzi di ricerca della prova" ovvero "momento acquisitivo della stessa"; si può osservare come i rilievi non siano in alcun modo identificabili con gli accertamenti.

Dopo aver definito il significato proprio degli accertamenti, è importante anche comprendere, il senso del termine "tecnico" riguardante quest'ultimi.

Il suddetto termine è chiarito direttamente dal codice di rito al comma 1 dell'art. 359 c.p.p., dal quale si deduce che la tecnicità dell'accertamento si pone in funzione della necessità dell'apporto di competenza specifica che il P.M o i suoi ausiliari non hanno.

Per questa ragione, il P.M., la P.G. ed anche la difesa, possono avvalersi della competenza specifica propria dei

---

30 Cass., Sez.I, 2 aprile 2009, n. 14511 reperibile sul sito www.guidaaldiritto.ilsole24ore.com.

31 S.SOTTANI, *Rilievi e accertamenti sulla scena del crimine,* in *Arch. pen,*2011, p.3.

32 C. TAORMINA, *Diritto processuale penale,* vol.I, 1995, p.254.

consulenti tecnici, i quali, è fondamentale che svolgano la loro attività, secondo elevati *standard* di "qualità e professionalità".

In verità, però, non sempre l'attività dei consulenti tecnici, può essere giudicata irreprensibile o esente da errori.

Basti osservare, in merito, i più gravi fenomeni di *junk science*[33], che appartengono ad una dimensione patologica della ricerca scientifica applicata all'accertamento giurisdizionale, dalla cui analisi, non può non rilevarsi che l'errore, costituisca una componente essenziale insita nella stessa natura umana[34].

Nel prosieguo dell'analisi delle definizioni terminologiche, rimane ancora da chiarire la distinzione tra accertamenti ripetibili e accertamenti irripetibili.

I primi, riguardano operazioni tecniche che hanno ad oggetto cose o luoghi, il cui stato non è soggetto a modificazione durante il loro espletamento; al contrario, i secondi, consistono in operazioni tecniche disposte su cose o luoghi, il cui stato è sottoposto a modificazione[35].

In quest'ultimo caso, l'art. 360 c.p.p., prevede una particolare procedura, volta a consentire idonee garanzie difensive, dispone infatti che: "il P.M. debba avvisare, senza ritardo, la persona sottoposta alle indagini, i difensori e la parte offesa, informandoli del giorno e dell'ora in cui verrà conferito

---

33 Tale termine indica una voluta distorsione dei metodi scientifici, al fine di raggiungere conclusioni che non sarebbero accettabili o confermate, se svolte tramite ricerche scientifiche corrette.

34 A.SPINELLA, G.SOLLA, *L'identificazione personale nell'investigazione scientifica: DNA e impronte,* in *Cassazione penale*, 2009, p. 435.

35 F.NOVARIO, *L'attività d'accertamento tecnico difensivo disposta su elementi informatici e la sua ripetibilità,* in Riv. *Ciberspazio e diritto,* 2011, p.76 ss.

l'incarico al consulente tecnico per lo svolgimento delle attività tecniche, con la facoltà dei chiamati, di nominare consulenti tecnici di parte oppure, formulare riserva di promuovere un incidente probatorio".

Sul concetto di "avviso senza ritardo" menzionato al 1°comma, ci si deve interrogare sulla sorte delle indagini informatiche, compiute senza che il medesimo venga apprestato[36].

A tal riguardo, non convince la tesi secondo la quale, si tratterebbe di accertamenti inutilizzabili nel senso stretto del termine[37].

Gli accertamenti non ripetibili integrano questo vizio, quando il P.M. li disponga nonostante risultino rinviabili e l'indagato si sia riservato di promuovere incidente probatorio. È in tale evenienza in cui è prescritto che i loro risultati non possano essere utilizzati nel dibattimento (art. 360 co. 5° c.p.p.).

Ciò non significa, che il mancato preavviso al difensore, rimanga sfornito di sanzioni.

La disposizione è senz'altro da ricollegare a quelle che riguardano "l'assistenza" dell'indagato, poiché è preordinata all'esplicazione del contraddittorio tecnico da parte della difesa, dunque la sua inosservanza, determina una nullità di genere intermedio (artt.178,lett. *c*, e 180 c.p.p)[38].

La nullità degli accertamenti tecnici non ripetibili, effettuati

---

36 M.DANIELE, *Il diritto al preavviso della difesa nelle indagini informatiche,* in Riv. *Cassazione penale* 2012, p.444.

37 L.LUPARIA, *Computer crimes e procedimento penale,* dal testo *Trattato di procedura penale. Modelli differenziati di accertamento,* a cura di G.Garuti, vol. VII, t.I, Utet 2011.

38 N.GALANTINI, *L'inutilizzabilità della prova nel processo penale,* Giuffrè, 1992, p.388.

senza preavvisare la difesa – come del resto ogni altra nullità di genere intermedio – si differenzia dall'inutilizzabilità, sotto il profilo dell'arco temporale di rilevabilità: non in ogni stato e grado del procedimento, ma entro i termini fissati dall'art. 180 c.p.p.

Ne discende che la nullità in questione, in quanto inerente alla fase investigativa, debba essere eccepita o rilevata prima della deliberazione della sentenza di primo grado[39].

L'effetto della nullità è, peraltro, circoscritto perché ha un raggio operativo limitato:

a) Non si riflette sugli ulteriori atti d'indagine e sui mezzi di ricerca della prova espletabili, nonché sulle prove reperibili grazie alle informazioni prodotte dai dati digitali invalidi.

b) In ogni caso, non impedisce la condanna quando esistono altre prove in grado di supportare il giudizio di colpevolezza.

c) Infine, non opera quando la prova digitale deve essere impiegata ai fini di un provvedimento che non ha ad oggetto la colpevolezza e neppure nell'ambito dei riti speciali senza dibattimento.

Rimangono escluse dalle ipotesi di cui all'art. 360 c.p.p, quelle attività di P.G. compiute *ex.* art. 354 c.p.p. qualora sia necessario svolgere "accertamenti urgenti" e conservare lo stato dei luoghi prima dell'intervento del P.M. esse, infatti, sono tutta una serie di operazioni atipiche da documentare con idoneo verbale.

---

39 M.DANIELE, *Il diritto al preavviso della difesa nelle indagini informatiche,* in *Cassazione penale,* 2012, p.445.

I.4.1 **Disquisizioni sulla natura ripetibile o irripetibile degli accertamenti tecnici informatici**

La l. 48/2008, ha apportato una rilevante modifica al 2° comma dell'art.354 c.p.p..

Essa si sostanzia nell'aver esteso le attività di conservazione, rilievi ed accertamenti, alla realtà informatica complessivamente intesa, spesso difficilmente riconducibile alle previgenti nozioni di "cose" o "luoghi".

Ciò posto, proprio in relazione al nuovo dato normativo, paiono intrecciarsi due problematiche: la prima, riguardante la possibilità per la P.G. di compiere attività valutative tecniche di propria iniziativa, la seconda, relativa alla natura ripetibile o irripetibile dell'accertamento "informatico"[40].

Quanto al primo *thema,* vi è convergenza di opinioni, laddove si conviene (e ciò anche anche prima della modifica apportata dalla l.48/2008), che l'oggetto esaminato dalla P.G., non possa essere modificato dalle operazioni dalla medesima esperite.

Con il voler specificare, che la P.G. sia incaricata di "assicurare la conservazione" dell'elaboratore, "d'impedirne l'alterazione e l'accesso" oltre che di effettuare "copie" non modificabili, sembra che il legislatore voglia ribadire che tale soggetto processuale, nell'ambito in questione, si limiti alle sole attività di assicurazione e preservazione del quadro probatorio[41].

---

40 S.ATERNO, *La fase di acquisizione degli elementi di prova digitale: attività irripetibile o ripetibile?,* (a cura di) S.Aterno, F.Cajani, G.Costabile, M.Mattiucci, G.Mazzarco, in *Computer forensics e Indagini digitali,* Experta 2001, p. 370

41 G.SPANGHER, *Trattato di procedura penale, vol. 3°. Indagini*

Riguardo la seconda problematica, invece, si è instaurato un acceso dibattito, su come debbano essere intesi gli accertamenti tecnici informatici, ovvero se essi siano atti aventi natura ripetibile o irripetibile.
Innanzitutto, bisogna specificare che le analisi forensi sono di varia natura e, per questo motivo, è difficile ricondurre tutte le operazioni di *forensics* in un'unica categoria tipologica.

Per renderne più agevole la comprensione, può risultare d'ausilio porre l'attenzione sull'analisi di un caso frequente e comune, ovvero l'estrazione di un dato dall' *hard disk* di un *pc* sottoposto a sequestro. Tale atto, secondo giurisprudenza consolidata, non può considerarsi atto irripetibile[42].

La Suprema Corte in merito, infatti, ha ritenuto che "la nozione di atto non ripetibile non ha natura ontologica, ma va ricavata dalla disciplina processuale, caratterizzata dal bilanciamento degli interessi tra la ricerca della verità nel processo e il sacrificio del principio costituzionale relativo alla formazione della prova nel contraddittorio tra le parti"; ancora, ha ritenuto "di escludere che l'attività di estrazione di un *file* da un *computer* costituisca un atto irripetibile, atteso che non comporta alcuna attività di carattere valutativo su base tecnico scientifica, né determina alcuna alterazione dello stato delle cose, tale da recare pregiudizio al contributo conoscitivo nella prospettiva dibattimentale, essendo sempre comunque assicurata la riproducibilità delle informazioni identiche a quelle contenute nell'originale".

---

preliminari e udienza preliminare, Utet giuridica, 2009, p. 234.
42 Sez.I, 5 marzo 2009, n. 14511, in *CED 243150.*

Tuttavia, non sono mancate le contestazioni da parte della dottrina[43] che hanno posto come obiezione, l'ineludibile rilievo secondo il quale ogni accesso ad un *file*, se effettuato erroneamente, comporta una modifica e/o alterazione di dati.
Si deve considerare, però, come il testo dell'art. 354 c.p.p., al secondo comma, prescriva che la P.G. possa effettuare un'immediata duplicazione su adeguato supporto.
Nella prassi, avviene infatti, che la Procura, dopo aver proceduto al sequestro del *pc*, effettui una copia dell'*hard disk* e poi, restituisca il tutto all'indagato: la Corte di Cassazione[44], ha affermato che tale procedura integri un atto ripetibile, proprio alla luce delle disposizioni in tema di sequestro della Polizia Giudiziaria.
Si legge appunto nella motivazione della più importante sentenza[45] sul tema: "la lettura dell'hard disk non integra affatto atto irripetibile, perché l'attività svolta al riguardo dalla P.G., rientra tra quelle svolte dalla stessa ai sensi dell'art. 348 c.p.p. ed art. 354 c.p.p. comma 2"; ed ancora: "correttamente invero, per l'estrazione dei dati contenuti nel supporto informatico - essendo l'accertamento all'evidenza ripetibile se eseguito, come *non è dubbio sia avvenuto nel caso di specie da personale esperto, perfettamente in grado di evitare la perdita dei dati medesimi* - è stato applicato l'art. 359 c.p.p. e non l'art. 360 c.p.p.".
A complicare lo scenario in relazione al delicato aspetto del programma utilizzato per l'estrazione dei *file,* parte della

43 P.TONINI, *Documento informatico e giusto processo*, in Riv. *Diritto penale e processo,* 2009 n. 405.
44 Cass. Sez. I, 16 marzo 2009, n. 11503, in *CED* 243495
45 Cass. Sez. I, 18 marzo 2009, n. 11863, in *CED* 243922.

dottrina[46] ha messo in risalto anche un altro dato, secondo cui, i programmi informatici utilizzati per le analisi forensi "sono quasi sempre coperti da licenza, in quanto commercializzati da grandi aziende informatiche. Ciò impedisce di poter accedere ai cc.dd. "codici sorgente", vale a dire alle vere e proprie fondamenta, che sorreggono l'intelaiatura del programma e ne condizionano il funzionamento".

Ne consegue che l'eccezione difensiva, che voglia far leva sulla impossibilità per giudice e avvocato, di esaminare il concreto funzionamento di quel programma e quindi, di poter monitorare la correttezza dell'*iter* da esso seguito, con conseguente garanzia di fedeltà della copia effettuata, parrebbe, quindi, del tutto fondata.

Secondo altri studiosi, però, tale affermazione risulta opinabile per più ragioni[47].

Prima di tutto molti dei programmi utilizzati dagli stessi indagati sono di tipo "proprietario"[48] e non è possibile accedere ai codici sorgente, ma non per questo si mette in discussione la rappresentazione di atti o fatti giuridicamente rilevanti, quando si utilizzano documenti informatici (ad es. *office word,* sul quale può essere apposta anche una firma digitale legalmente riconosciuta dalla normativa italiana).

---

46 L.LUPARIA, G.ZICCARDI, *Investigazione penale e tecnologia informatica,* Milano 2007, p.152ss.

47 S.ATERNO, *La fase di acquisizione degli elementi di prova digitale: attività irripetibile o ripetibile?,* (a cura di) S.Aterno, F.Cajani, G.Costabile, M.Mattiucci, G.Mazzarco, in *Computer forensics e Indagini digitali,* Experta 2011, p. 373

48 La definizione di formato proprietario in informatica è riferita a qualsiasi formato di *file* di cui non siano note le specifiche tecniche. Solitamente le specifiche tecniche sono ritenute proprietà intellettuale della persona, dell'organizzazione, dell'azienda che ha sviluppato il *file.*

Altro aspetto da non sottovalutare è che, comunque, le analisi condotte dal NIST[49] hanno portato a definire qualitativamente affidabili strumenti di analisi forense nelle varie versioni.

In ogni caso queste importanti *software house* sono disponibili a fornire il codice sorgente al giudice, mediante una sorta di accordo di segretezza per le eventuali attività peritali volte all'analisi del comportamento di tali strumenti informatici.

Da quanto detto, emerge uno scenario in cui, le garanzie difensive appaiono fortemente limitate.

Se le operazioni di estrazioni dei *file* vengono considerate, come spesso accade, atti aventi natura ripetibile e, quindi, le operazioni sui dati effettuati senza le garanzie previste dal 360 c.p.p., l'attività difensiva si limita ad una attività *post mortem* (ovvero su sistema spento o scollegato), con un supporto dal quale sono estratti dati estrapolati da soggetti, dei quali si deve sempre presumere la competenza.

Tuttavia la cronaca giudiziaria italiana ci ha recentemente insegnato, con il caso Garlasco[50], che la scena "informatica" del crimine può ben essere compromessa dagli operanti di Polizia Giudiziaria.

A tal proposito, però, il difensore ha sempre una possibilità difensiva, qualora il *computer* sia in sequestro e non sia stato disposto un accertamento tecnico *ex* art. 360 c.p.p., ovvero di richiedere, *ex* art. 233 co. 1-*bis* c.p.p.[51], l'effettuazione di una

49 *Nascional Institute of Standards and Tecnology* che, con un progetto specifico chiamato *Computer Forensic Tool Testing* (CFTT), effettua test approfonditi di *hardware e software*

50 Cfr. *Validità delle "Malpractices" nell'ordinamento e sentenze giurisprudenzali a confronto,* v. infra cap. 2, par. II.6

51 Art. 233, co. 1 *bis,* c.p.p., "*Il giudice, a richiesta del difensore, può*

consulenza tecnica assolutamente autonoma sulla copia dei dati estratti.

Degno ancora di nota appare il profilo secondo cui il P.M. nell'assumere la scelta se effettuare un accertamento ai sensi dell'art. 360, deve valutare, da un lato, le circostanze del caso concreto e, dall'altro, le implicazioni procedurali[52]. Procedere secondo questi criteri, "mette al riparo" da eventuali eccezioni difensive dibattimentali, in relazione all'inutilizzabilità di quanto raccolto in fase di indagini, se ritenuto atto irripetibile.

Al riguardo, non sono mancati casi in cui il P.M. ha deciso di procedere *ex* art. 360 per ragioni di mera opportunità.

Un esempio[53] in tal senso, è quella assunta dalla procura di Milano in data 12 luglio 2006, in relazione agli accertamenti effettuati sull'archivio informatico del SISMI[54], nell'indagine relativa al rapimento di Abu Omar: attesa la presenza di un archivio contenente numerosissimi *files*, molti dei quali crittografati[55], il Pubblico Ministero decise di procedere ai

---

autorizzare il consulente tecnico di una parte privata ad esaminare le cose sequestrate nel luogo in cui si trovano, ad intervenire alle ispezioni, ovvero ad esaminare l'oggetto delle ispezioni alle quali il consulente non è intervenuto. Prima dell'esercizio dell'azione penale l'autorizzazione è disposta dal pubblico ministero a richiesta del difensore".

52 S.ATERNO, *La fase di acquisizione degli elementi di prova digitale: attività irripetibile o ripetibile?,* (a cura di) S.Aterno, F.Cajani, G.Costabile, M.Mattiucci, G.Mazzarco, in *Computer forensics e Indagini digitali,* Experta 2011, p. 386.

53 F.SANSA, C.ZAGARIA, *Caccia ai file nell'ufficio Sismi. I pm avviano la perizia sui pc,* in *La Repubblica,* 14 luglio 2006, reperibile sul sito www.repubblica.it.

54 Il *SISMI*, (Servizio informazioni e Sicurezza militare), è stato un servizio segreto italiano, di natura militare, in attività fino alla riforma normativa del 2007, quando fu sostituito dall'Agenzia informazioni e sicurezza esterna, c.d. AISE.

55 La *Crittografia,* è un metodo che viene utilizzato per rendere un messaggio offuscato, al fine di non essere compreso da persone non autorizzate a leggerlo.

sensi dell'art 360 c.p.p. anche se nella richiesta dell'atto motivava "pur potendosi considerare ripetibili gli accertamenti in questione, appare opportuno, procedere *ex* art. 360 c.p.p., onde prevenire possibili questioni procedurali"[56].

Appare necessario, dunque, collocare la natura di irripetibilità dell'atto, al momento e al caso specifico nel quale esso viene svolto.

Tale assunto dipende dalla tipologia del sistema informatico (*server* o semplice *computer*) dal suo stato (acceso o spento) e dal momento "storico" delle attività investigative.

Da ultimo, si evidenzia come l'unico caso nel quale si può presumere che i dati estratti con copia forense restino pressoché inalterati sia l'ipotesi già accennata, di un' analisi "*post mortem*"; nei sistemi ancora attivi (anche in stato di *stand-by*), infatti, ogni operazione effettuata comporta, almeno potenzialmente, una modificazione dei dati.

Ovviamente, non si vuole arrivare a sostenere che l'attività di copia o apprensione dei dati digitali sia azione sempre e comunque irripetibile quanto, piuttosto, che sia necessario appurare le modalità con le quali viene svolta, nell'ottica di una piena trasparenza e verificabilità[57].

Da qui la necessità di contemperare, nel singolo caso, le esigenze di conservazione della fonte di prova e le garanzie difensive dell'indagato, sulla scia dell'insegnamento sempre valido secondo cui, fondamento del processo penale rimane,

56 S.ATERNO, *La fase di acquisizione degli elementi di prova digitale: attività irripetibile o ripetibile?,* (a cura di) S.Aterno, F.Cajani, G.Costabile, M.Mattiucci, G.Mazzarco, in *Computer forensics e Indagini digitali,* Experta 2011, p. 387

57 L.LUPARIA, *Processo penale e tecnologia informatica,* in Riv. *Diritto dell'Internet* 2008, p.221.

quali che siano le evoluzioni della scienza e della tecnica ed i mutamenti sociali e culturali, il rispetto della persona umana e della sua dignità.

CAPITOLO 2
I MEZZI DI RICERCA DELLA *DIGITAL EVIDENCE*

II.1 I mezzi di ricerca della prova nel codice di procedura penale

Nell'attuale sistema di diritto processuale penale, il procedimento di formazione della prova si articola in quattro fondamentali fasi: ricerca, individuazione, acquisizione (momenti afferenti all'accertamento della verità materiale) e valutazione della prova (momento afferente al convincimento del giudice).

L'adesione al sistema accusatorio ed al principio dialettico della prova, infatti, ha disegnato un sistema in cui l'accertamento della verità processuale deve necessariamente articolarsi nella ripartizione delle funzioni processuali tra soggetti portatori di interessi contrapposti[58].

Il codice di procedura penale definisce "mezzi di ricerca della prova" quegli strumenti di indagine che costituiscono il mezzo attraverso il quale la prova si assume: ispezioni,

58 P.TONINI, Manuale di procedura penale , Giuffrè Editore, 2012, p. 211 e ss.

perquisizioni, sequestri ed intercettazioni di comunicazioni.

Mediante tali strumenti è possibile l'acquisizione al dibattimento della fonte di prova ed, in fase dibattimentale, la prova vera e propria[59].

Nella Relazione al progetto preliminare del codice di procedura penale è ben delineata la differenza tra mezzi di prova e mezzi di ricerca della prova.

I primi hanno l'attitudine ad offrire al giudice, nella fase di valutazione, risultanze probatorie direttamente utilizzabili in sede di decisione.

I mezzi di ricerca della prova, al contrario, non costituiscono di per sé fonte di convincimento, ma rendono possibile l'acquisizione di cose materiali, tracce o dichiarazioni dotate di attitudine probatoria[60].

Tali strumenti sono quindi atti a veicolare innanzi al giudice fonti del suo convincimento che preesistono e, che sono acquisite quasi sempre in fase di indagini preliminari.

Di qui la fondamentale differenza: i mezzi di prova sono creativi della prova stessa nel dibattimento (tranne che nel caso, del tutto peculiare, dell'incidente probatorio); i mezzi di ricerca della prova operano essenzialmente prima della formazione della prova, nella summenzionata fase di ricerca.

Fondamentale è la differenza anche per quanto attiene al procedimento con cui sono disposti.

Mentre la disposizione dei mezzi di prova avviene con ordinanza del giudice (d'ufficio o su istanza di parte), i mezzi di ricerca della prova sono disposti con decreto motivato

---

59 M. PISANI et alii, Manuale di procedura penale, 8a ed., Bologna, Monduzzi, 2008, pag 227 e ss.

60 P.TONINI, Manuale di procedura penale , cit. p. 373

dell'autorità giudiziaria, ed è quindi espressione anche dell'ufficio del Pubblico Ministero.

Anche il P.M. può quindi disporre dei mezzi di ricerca della prova, spesso caratterizzati dal requisito della "sorpresa"[61], non consentendo il preventivo avviso al difensore.

Per meglio comprendere quanto seguirà nel corso di questa trattazione, può essere d'ausilio procedere ad una prima analisi sommaria dei diversi mezzi di ricerca della prova così come delineati dal codice di procedura penale.

L'ispezione (art. 244 c.p.p.) consiste nell'attività di osservare e descrivere persone, luoghi e cose allo scopo di accertare le tracce e gli altri effetti materiali del reato: è infatti definita tradizionalmente come "osservazione giudiziale immediata"[62].

Si deve rilevare che il codice di procedura penale prevede diverse garanzie per la persona sottoposta alle indagini preliminari in fase di ispezione: il diritto di difesa si articola infatti in due alternative facoltà per il difensore.

In *primis*, quella di assistere allo svolgimento dell'atto ispettivo, se si tratta di atto cui stia procedendo di sua iniziativa la Polizia Giudiziaria, che è pertanto classificato come atto assolutamente urgente.

Nei casi di non assoluta urgenza, invece, sia che proceda il Pubblico Ministero, sia che proceda l'ufficiale di Polizia Giudiziaria delegato, il difensore deve essere preventivamente avvisato.

Il codice di procedura penale prevede altresì per la persona sottoposta alle indagini la facoltà di farsi assistere da persona

61 M. PISANI et alii, Manuale di procedura penale, 8a ed., pag. 227ss.
62 ibidem

di sua fiducia.

Tali garanzie si estendono anche all'ispezione di sistemi informatici, che inoltre deve essere eseguita, come si avrà modo di approfondire *infra*, previa adozione di adeguate cautele tecniche.

Per quanto attiene ai fini del presente elaborato, si deve rilevare che proprio per quanto attiene all'ispezione del dato informatico, assume rilievo il dettato dell'art.244 comma 2 così come modificato dall'intervento normativo del 2008.

Se il reato, infatti, non ha lasciato tracce o effetti materiali (o se questi sono scomparsi), l'autorità giudiziaria deve cercare di individuare il modo, il tempo e le cause delle eventuali modificazioni[63].

Procedendo nell'analisi, la perquisizione è un mezzo di ricerca della prova analogo a quello appena descritto dell'ispezione, ma che da esso va tenuto distinto, sebbene soprattutto nell'ambito informatico, come si avrà modo di approfondire in seguito[64], la distinzione possa essere tutt'altro che agevole.

La perquisizione consiste nell'attività volta ad acquisire al processo il corpo del reato e le cose pertinenti al reato, cioè quelle cose sulle quali o a mezzo delle quali il reato è stato commesso, e quelle che ne costituiscono il profitto, il prezzo, il prodotto o un mezzo di prova (art. 253 co.2 c.p.p.).

È in questo che si deve rinvenire il profilo fondamentale di distinzione con l'ispezione: mentre con quest'ultima si ricercano tracce o effetti materiali del reato, con la perquisizione si ricercano il corpo del reato, cose pertinenti

63 P.TONINI, Manuale di procedura penale , cit. p. 376
64 Cfr. par. II.3.2

allo stesso o persone.

In punto di difesa tecnica, parallelamente a quanto si è riferito *supra* circa l'ispezione e le facoltà del difensore, quest'ultimo ha sempre diritto di assistere ai vari tipi di perquisizione, anche se posti in essere in situazioni di urgenza dal Pubblico Ministero o dalla Polizia Giudiziaria (artt. 356 e 365 c.p.p.).

Si deve rilevare che, invece, la natura di atto a sorpresa esclude l'obbligo di preavviso al difensore per le perquisizioni.

Per quanto attiene al sequestro, il codice di rito ne prevede tre distinte forme: il sequestro preventivo e quello conservativo sono collocati tra le misure cautelari.

Nella nostra analisi è necessario soffermarsi sul sequestro cosiddetto probatorio di cui all'art. 253 e seguenti del codice di procedura penale, che costituisce un mezzo di ricerca della prova.

Comune ai tre tipi di sequestro summenzionati è la caratteristica di creare un vincolo di indisponibilità sulla cosa, mobile o immobile, che investono, attraverso una procedura coattiva di spossessamento[65].

Nel caso del sequestro probatorio, il vincolo è finalizzato a conservare immutate le caratteristiche della cosa per finalità probatorie, ovverosia per procedere all'accertamento dei fatti nel procedimento penale.

Il sequestro probatorio, infatti, è il mezzo di ricerca della prova attraverso il quale l'autorità giudiziaria, con decreto motivato, dispone che venga acquisito il corpo del reato o le

65 P.TONINI, Manuale di procedura penale , cit. p. 380

cose attinenti al reato che siano necessari ai fini dell'indagine in corso.

È rilevante sottolineare che in genere il sequestro è consequenziale rispetto alla previa perquisizione, scaturendo appunto da una fase dell'indagine diretta ad acquisire il corpo del reato e le cose ad esso pertinenti.

Differenza fondamentale ed intuitiva tra perquisizione e sequestro è che la prima attiene all'attività di ricerca, il secondo alla fase di immediata acquisizione.

Interessante è osservare come, anche sul punto in esame, le strutture classiche del diritto processuale penale possono risultare insufficienti.

In base ad una certa impostazione tradizionale, infatti, si riteneva che, ai fini del sequestro probatorio, fosse necessario un requisito naturalistico della cosa, ossia che si trattasse di un bene materiale.

In base a tale orientamento, infatti, la norma sul sequestro probatorio risulta inapplicabile per creare vincoli rispetto a posizioni giuridiche soggettive o a beni immateriali, potendosi ad essi applicare invece sequestro conservativo o sequestro preventivo[66].

Sul punto, e come si avrà modo di approfondire di seguito nell'analisi del sequestro probatorio di dati informatici, dottrina e giurisprudenza appaiono divise.

Le critiche più articolate, da parte della dottrina, hanno preso le mosse da un attento esame dell'istituto: l'art. 253 comma 2 c.p.p. indica quale corpo del reato, quelle cose sulle quali o mediante le quali il reato è stato commesso, con inclusione

66 Ibidem

altresì di quelle che ne costituiscono il prodotto, il profitto o il prezzo.

Secondo la citata dottrina, non sarebbe conciliabile la definizione marcatamente materiale del sequestro probatorio adottata dal legislatore con la natura immateriale delle tracce informatiche[67].

Infine, strumento ampiamente diffuso per la ricerca della prova è quello delle intercettazioni.

Il codice di procedura penale non definisce lo strumento delle intercettazioni

Lo strumento dell'intercettazione è stato definito dalla Corte di Cassazione come l'attività di "captazione occulta e contestuale di una comunicazione o conversazione tra due o più soggetti che agiscano con l'intenzione di escludere altri e con modalità oggettivamente idonee allo scopo".

La captazione deve essere attuata "da un soggetto estraneo alla conversazione, mediante strumenti tecnici di percezione tali da vanificare le cautele ordinariamente poste" a protezione del carattere riservato della conversazione stessa[68].

Pertanto, non può ritenersi che costituisca attività di intercettazione - e dunque non può ritenersi mezzo di ricerca della prova così enucleato - l'attività di registrazione di un colloquio effettuata clandestinamente da chi partecipi ad esso.

Quanto all'*ubi consistam*, le intercettazioni possono consistere in acquisizione di conoscenza di

67 G.COSTABILE, Scena criminis, documento informatico e formazione della prova penale, in www.penale.it

68 Cass.Pen. sez. VI n. 12189/2005

telecomunicazioni telefoniche (mediante telefono o altre forme di trasmissione), nonchè di colloqui tra presenti all'insaputa di almeno uno dei coinvolti nella conversazione (cosiddette intercettazioni ambientali).

Ai sensi dell'articolo 266 bis c.p.p., sono inoltre consentite le intercettazioni del flusso di comunicazione relativa sistemi informatici o telematici: “nei procedimenti relativi ai reati indicati nell’articolo 266, nonché a quelli commessi mediante l’impiego di tecnologie informatiche o telematiche, è consentita l’intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi”.

La richiesta di utilizzare le intercettazioni è presentata dal Pubblico Ministero ed è autorizzata dal GIP con decreto motivato, quando vi sono gravi indizi di reato e l’intercettazione è assolutamente indispensabile ai fini della prosecuzione delle indagini.

Nei casi di urgenza, il decreto motivato è disposto dal Pubblico Ministero e comunicato immediatamente, o comunque non oltre le 24 ore, al Giudice per le indagini preliminari.

Dopo aver fornito un breve quadro generale, senza pretese di completezza, sul tema dei mezzi di ricerca della prova nel sistema processuale penale vigente, si procederà all’analisi delle peculiarità di tali mezzi nell’ambito della prova digitale.

II.2 I mezzi di ricerca della prova digitale: L'ispezione e la perquisizione dei dati informatici.

La l. 48/2008 ha integrato il testo degli articoli 244 e 247 c.p.p., per consentire esplicitamente il compimento di ispezioni e perquisizioni su sistemi informatici e telematici.

In particolare l'autorità giudiziaria, al fine di rilevare eventuali tracce digitali lasciate nella consumazione del reato, ovvero se tali tracce non siano state lasciate ma cancellate, disperse, alterate o rimosse, potrà compiere oltre i soliti rilievi descrittivi e fotografici, ogni altra operazione tecnica su sistemi informatici o telematici.

Inoltre, potrà svolgere perquisizioni sui medesimi sistemi, ancorché protetti da misure di sicurezza, quando vi sia fondato motivo di ritenere che in essi si trovino dati, informazioni, programmi informatici o tracce comunque pertinenti al reato[69].

Sia in ambito di ispezione che di perquisizione, viene offerto un "paradigma" sul corretto *modus operandi* da seguirsi nelle operazioni di accesso al *computer* oggetto d'indagine, con particolare attenzione alla "salvaguardia dell'integrità dei dati digitali" che assume, quindi, canone operativo imprescindibile.

Nel testo di legge in esame, infatti, è posto di sovente l' interesse sulla necessità di adottare "misure tecniche idonee dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione".

La precisazione in analisi è posta a sostegno di un duplice

69 A. VITALE, *La nuova disciplina delle ispezioni e delle perquisizioni in ambiente informatico o telematico,* in *Dir. dell'Int.,* 2008, p. 503.

obiettivo: da un lato, garantire la genuina acquisizione di elementi probatori che potranno assumere successivamente valenza di prova; dall'altro, sul fronte delle garanzie difensive, permettere un controllo sull'operato degli inquirenti che deve necessariamente prendere le mosse dalla verifica sulle procedure acquisitive.

Si è osservato che la locuzione[70] sopra richiamata, appaia come "norma processuale in bianco" attraverso un implicito richiamo alle *best practices* del settore, senza però indicare a quale fra le molteplici esistenti ci si debba riferire.

Il legislatore mostra una certa indifferenza fra le plurime procedure, lasciando margine d'azione e di scelta al *forenser* che concretamente porrà in essere le operazioni secondo la tecnica preferita, sempre che il risultato acquisito rispetti gli obiettivi della formula normativa di cui sopra[71].

Come si è avuto modo di descrivere nel precedente paragrafo, l'attività tipica dell'*inspicere* si sostanzia nell'osservazione di persone, luoghi, cose e nell'accertamento di tracce o altri effetti materiali del reato (art. 244, comma 1°).

Di contro, l'attività tipica del *perquirere* si caratterizza nell'individuazione e acquisizione del corpo del reato o delle cose ad esso pertinenti, spesso qualificandosi come attività prodromica rispetto al sequestro probatorio (art. 247, comma 1°).

Quello su cui appare doveroso porre l'attenzione, è la *ratio*

---

70 "misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione".

71 G.BRAGHO', *L'ispezione e la perquisizione di dati, informazioni e programmi informatici,* in *Sistema Penale e Criminalità Informatica,* a cura di L.Lupària, Giuffrè, 2009, p. 193.

per la quale il Legislatore abbia voluto novellare tali disposizioni.

Le motivazioni sono da rinvenire innanzitutto nell'esigenza di creare un *corpus* omogeneo di norme in tema di criminalità informatica, che rappresenta l'asse portante della Convenzione di Budapest: in tal modo il legislatore ha riconosciuto la specificità del settore d'indagine al quale è stato attribuito il nome di "*digital evidence*".

In secondo luogo, si deve evidenziare che le innovazioni legislative definiscono l'oggetto del mezzo di prova, le disposizioni in tema di ispezione e di perquisizione informatica fanno infatti esplicito riferimento a dati, informazioni, programmi e sistemi informatici.

Si deve sottolineare, infine, che il legislatore si è preoccupato in modo particolare di richiamare l'esigenza normativa di assicurare la conservazione dei dati originali e di impedirne l'alterazione (art.244, comma 2).

È quello da ultimo citato il *fil rouge* che lega tutte le modifiche normative in tema di ispezione, perquisizione e sequestro probatorio: "assicurare, mediante la corretta conservazione dei dati originali, la ripetibilità dell'accertamento investigativo in sede dibattimentale, ove si estrinseca con pienezza il contraddittorio fra le parti"[72].

Dalla conclusione cui si è appena pervenuti possono evincersi due corollari di notevole importanza.

In primo luogo, la qualificazione dell'attività ispettiva o perquisente in ambiente virtuale, come attività

72 G. BRAGHO', *L'ispezione e la perquisizione di dati, informazioni e programmi informatici,* in *Sistema Penale e Criminalità Informatica,* a cura di L.Lupària, Giuffrè 2009.

potenzialmente e concretamente idonea a modificare in maniera irreversibile lo stato e il contenuto interno del dispositivo sottoposto alla misura.

In secundis, il riconoscimento della "natura ontologicamente volatile e alterabile del dato digitale, su cui possono spesso incidere condotte involontarie atte a ingenerare fenomeni di inquinamento e la conseguente necessità di impiegare *standard operatin*g, ossia procedure idonee a garantire la genuinità dell'accertamento"[73].

II.3.2 **Il labile confine tra ispezione e perquisizione in ambito informatico**

Adattare però l'ispezione e la perquisizione di stampo tradizionale "all'ambiente virtuale" su cui andranno ad operare non è sempre agevole, soprattutto sotto il profilo tecnico.

Le attività in esame possono infatti sostanziarsi, in tale settore, in procedure essenzialmente analoghe, che rischiano di far sfumare in concreto la linea di demarcazione fra i due istituti.

Posto che, come detto, l'attività ispettiva è diretta alla ricerca visiva volta all'individuazione di tracce o effetti materiali del reato, bisogna domandarsi in quali termini sia possibile parlare di ispezione informatica e quali possano essere le modalità attuative.

In ambito informatico, esplorare un sistema alla ricerca di

---

73 L. LUPARIA, *I profili processuali,* in *Dir. pen. proc.,* 2008, p.719.

dati e tracce informatiche concernenti i fatti oggetto dell'ispezione, comporta irrimediabilmente l'alterazione dei dati di sistema e dei metadati relativi ai *file* oggetto di attenzione da parte degli inquirenti.

Parte della dottrina[74] ha infatti sottolineato come l'attività ispettiva in ambiente informatico dovrebbe limitarsi ad osservare il sistema descrivendolo nei suoi particolari, ad esempio rilevando la presenza di periferiche collegate, accesso alla rete attivo, presenza di software in funzione, partizioni logiche nascoste e rese visibili da meccanismi di autorizzazione connessi allo status dell'utilizzatore (ad esempio amministratore di sistema e chiavi di cifratura).

Altri invece[75], ne incoraggiano l'utilizzo, soprattutto con riguardo a reati di lieve entità (ad esempio diffamazione a mezzo *Internet*, diffusione di *virus*) o per casi dove è necessario acquisire solo una piccola parte dei dati contenuti nei dispositivi, dato che il sequestro dell'intero contenuto rappresenta un'operazione non rispondente al principio di proporzionalità con riguardo al fine (ad esempio nei casi di acquisizione presso terzi di dati rilevanti).

Si osserva come questa possibilità soffra comunque di due limiti importanti: il primo, di natura temporale, legato all'impossibilità di poter analizzare in maniera appropriata grande quantità di dati, tralasciandone giocoforza l'accuratezza e completezza; il secondo, invece, legato al rispetto delle garanzie difensive.

---

74 S. ATERNO, *Modifiche al titolo III del terzo libro del codice di procedura penale*, in *Cybercrime, responsabilità degli enti, prova digitale*, a cura di G. Corasaniti, G. Corrias Lucente, CEDAM, 2008, p. 206 e ss.

75 G. COSTABILE, *Scena criminis, documento informatico e formazione della prova penale*, in *Dir. inf. e informatica.*, 2005, p. 531

Rientrando, infatti, nella categoria degli accertamenti irripetibili, le operazioni ispettive dovranno rispondere allo schema previsto dall'art. 360 c.p.p.

Sebbene l'accertamento debba essere condotto da operatori tecnici appartenenti alla P.G. in contraddittorio con la parte interessata, eventualmente alla presenza di consulenti tecnici di parte, i risultati così ottenuti saranno cristallizzati in verbali con la conseguente utilizzabilità piena in dibattimento.

Resta preclusa la possibilità da parte dell'indagato di esperire *ex post* una nuova analisi sugli stessi supporti e sullo stesso oggetto, in quanto i risultati saranno necessariamente diversi, stante la modificazione dell'ambiente operata anteriormente dal *cyber* investigatore.

In realtà, poiché prevalgono le finalità di descrizione e rilevazione di dati oggettivi relativi al bene oggetto di ricerca, l'ispezione finalizzata all'acquisizione condotta *ex* art. 360 c.p.p. appare una via non praticabile, dovendosi quindi preferire la prima soluzione.

Ad avallare tale tesi è altresì il dato normativo che individua nel sistema informatico o telematico l'ambito di intervento ispettivo, più ampio rispetto alla disciplina della perquisizione che invece si rivolge a dati, informazioni o programmi: la *ratio* della norma sembra infatti rimarcare il fine ultimo delle attività dato dall'osservazione del sistema e dall'accertamento in ordine all'esistenza nel sistema di determinate applicazioni.

II.3 **La *preview* dei reperti**

Il panorama appena delineato si complica ulteriormente nel caso di utilizzo della c.d. "*preview* dei reperti"[76]: attraverso l'utilizzo di cc.dd. *software ad hoc* viene permesso agli inquirenti di analizzare preliminarmente il contenuto di un dispositivo per poi scegliere il materiale interessante e, se del caso, procedere a sequestro del dato.

E' da rilevarsi che questo può avvenire in sede d'ispezione, ma anche di perquisizione: fattore, questo, che alimenta ulteriormente la "confusione applicativa" fra i due istituti.

Si osserva, tuttavia, come tale operazione debba essere condotta da personale altamente qualificato, stante l'alto rischio di alterazione dei contenuti con conseguente dispersione di una possibile prova e, altresì, debba essere valutata caso per caso, non rappresentando ad oggi operazione di *routine* applicabile indiscriminatamente a qualsiasi fattispecie concreta.

A tal proposito sono interessanti le osservazioni di parte della dottrina, che ne suggerisce un uso attento e calibrato a seconda dell'indagine in essere: ad esempio, se si procede per il caso di pedopornografia *online*, sarà rilevante il materiale detenuto con dolo (presente e non cancellato) all'interno della memoria, per cui la *preview* potrebbe rappresentare un'opportunità utile al fine di evitare il sequestro di materiale non interessante rispetto al reato per cui si procede.

---

76 S. ATERNO, *Nozioni ed elementi tecnici di principio,* in *Computer forensics e indagini digitali. Manuale tecnico giuridico e casi pratici, Experta* 2011.

Diverso, invece, il discorso relativo ad indagini per stabilire un c.d. alibi informatico o, dove si renda necessario analizzare anche i *file* cancellati o di sistema.
In tali casi sarà opportuno sequestrare tutto il materiale contenente dati, per poter ricostruire le attività poste in essere dal *computer* e sul medesimo, quindi in questa ipotesi, lo strumento della *preview* appare inidoneo ai fini dell'accertamento.

II.3.4 **La perquisizione digitale: profili di incostituzionalità**

In merito al mezzo della perquisizione, come noto, può prodursi in sede d'indagini preliminari a seguito di due distinte modalità: solitamente, avviene d'iniziativa del Pubblico Ministero, il quale, attraverso decreto motivato la dispone prevedendo altresì se eseguirla personalmente o delegarla agli ufficiali della Polizia Giudiziaria(art. 247 c.p.p.).
Può però accadere che, sempre in sede d'indagini preliminari, la P.G. possa dar luogo personalmente e di propria iniziativa, a perquisizione locale o personale nei casi di flagranza del reato o evasione (art. 352 c.p.p.).
In quest'ultimo caso, essendo la perquisizione atto coercitivo potenzialmente lesivo dei diritti costituzionali di cui agli articoli 13 e 14 della Costituzione, necessita, *ex post*, di convalida da parte del P.M. entro le 48 ore successive per accertarne il fondamento: in caso contrario, i risultati così ottenuti e cristallizzati all'interno del verbale di perquisizione

saranno inutilizzabili.

Con la previsione di cui al nuovo comma 1-*bis* dell'art. 247 c.p.p., il legislatore stabilisce più invasivi poteri da parte degli investigatori, prevedendo altresì che "quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione".

Il punto relativo alle misure di sicurezza rende ancor più garantita la figura del "domicilio informatico" alla quale sembrano estendersi tutte le garanzie previste al "domicilio tradizionale"[77].

In parallelo attraverso la modifica all'art. 354 c.p.p. si prevede, in tema di accertamenti urgenti da parte della P.G., che la stessa, prima dell'intervento del Pubblico Ministero sia tenuta alla conservazione dello stato dei luoghi e delle cose pertinenti al reato (1° comma) e, in relazione a dati, informazioni, programmi, sistemi informatici o telematici sia tenuta all'adozione di misure tecniche o prescrizioni necessarie ad assicurarne la conservazione, impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità (2° comma).

In sostanza, nell'ambito delle attività in questione dovrà

77S.ATERNO, *Aspetti giuridici comuni delle indagini informatiche,* in *Computer forensics e indagini digitali. Manuale tecnico giuridico e casi pratici, Experta* 2011.

limitarsi a porre in essere azioni volte alla preservazione e assicurazione del quadro probatorio originario.

Ciò che è importante sottolineare, essendo attività prodromica rispetto al sequestro, è la necessità a che la perquisizione, anche in via informatica, sia opportunamente giustificata e legata al *thema probandum*, attraverso l'individuazione del fatto storico, di natura penalmente rilevante, in cui assume importanza e decisività l'elemento informatico.

In mancanza, non sarebbe possibile accertare l'esigenza probatoria sottesa al provvedimento, né la riconduzione del dispositivo a corpo del reato o cosa ad esso pertinente: si ravviserà quindi non più un mezzo di ricerca della prova bensì uno strumento discutibile di ricerca di notizie di reato.

Un'importante possibilità è appunto resa dalla *preview* dei reperti, come sottolineato in precedenza.

In ogni caso tali attività, sia di *preview* sia perquisenti in senso stretto, dovranno essere condotte con le cautele previste dall'art. 247, comma 1-*bis* c.p.p.: potranno consistere in operazioni differenti a seconda dello scenario che concretamente si manifesterà agli occhi degli inquirenti.

Diverso, infatti, è il trattamento tecnico da riservare a dispositivi rinvenuti in modalità *off* o *on*.

Si pensi al caso di ritrovamento sulla scena del crimine di due *computer*, di cui solo uno acceso.

Nel caso di computer spento, gli inquirenti qualora lo ritengano necessario, potranno esaminarne preliminarmente il contenuto e procedere eventualmente al sequestro dell'intero *hard-disk* o di alcune parti, attraverso il ricorso

alle procedure previste: ciò che preme rilevare è che in tale ipotesi, il rischio di alterabilità dei dati presenti è più basso rispetto al caso opposto, sempreché, in via preliminare, siano adottate le cautele previste dalle *best practices.*

La questione risulta invece più complessa nel caso in cui il dispositivo sia acceso e collegato alla rete: in questa ipotesi la prescrizione prevista dall'art. 247, comma 1-*bis* c.p.p. acquista un peso e una rilevanza ancor più imprescindibile, stante l'alto tasso di vulnerabilità del sistema dato dalla sua dinamicità.

Nell'affrontare un discorso sulla configurabilità della perquisizione *on line* come mezzo atipico di ricerca della prova, fondamentale è infine considerare il dettato di cui agli artt. 13-15 della Costituzione, che consente sì la compressione dei diritti inviolabili ivi sanciti, ma limitatamente ai casi e modi stabiliti dalla legge, fissando una duplice riserva di legge e di giurisdizione[78].

Precipitato logico è che la normativa processuale disciplinante i mezzi di ricerca della prova, non è altro che l'attuazione della duplice riserva, dato che provvede a fissare casi e modalità di restrizione della libertà personale, dell'inviolabilità domiciliare e della libertà e segretezza delle comunicazioni. Rimangono precluse interpretazioni estensive e analogiche, pena il travolgimento della legalità probatoria.

Il nostro ordinamento consente l'ingresso nel processo di prove atipiche, purché subordinate alle garanzie fissate nell'art 189 c.p.p., la cui collocazione sistematica ne consente l'applicabilità anche alla fase processuale, quella cioè

78G.BONO, *Il Divieto di indagini ad explorandum include i mezzi informatici di ricerca della prova,* in *Cass. pen.* 2013, p.1526

preposta alla verifica dell'ipotesi accusatoria incarnata dalla notizia di reato.

Il punto è che le perquisizioni *on line,* consentono agli organi inquirenti di accedere ai sistemi informatici e telematici dando luogo ad un monitoraggio dell'attività ivi realizzata ovvero alla clonazione in tempo reale dei dati digitali, ovviamente all'insaputa dell'utilizzatore[79].

Pur essendo astrattamente ammissibili, tuttavia i mezzi atipici di ricerca della prova non possono travolgere beni giuridici costituzionalmente protetti da riserva di legge, cadendo altrimenti nella sanzione dell'inammissibilità.

Ed è proprio tale sorte che attenderebbe la perquisizione *on line* ove si tentasse di ricorrervi, poiché malgrado la sua corrispondenza alle recenti esigenze probatorie, è incompatibile con il nostro ordinamento per contrasto alla sopra citata riserva di legge[80].

II.4 Il sequestro probatorio informatico

Il Sequestro probatorio è un mezzo tipico di ricerca della prova, disciplinato dagli articoli 253-265 del c.p.p., la cui funzione è quella di "assicurare una cosa mobile o immobile al procedimento per finalità probatorie, mediante lo spossessamento coattivo della cosa o la creazione di un vincolo di indisponibilità sulla medesima".

79 F.IOVENE, *Le c.d. Perquisizioni online tra nuovi diritti fondamentali ed esigenze di accertamento penale,* in *www.dirittopenalecontemporaneo.it*

80 G.BONO, *Il Divieto di indagini ad explorandum include i mezzi informatici di ricerca della prova,* in *Cassazione Penale* 2013, p. 1528

Il sequestro probatorio è generalmente disposto con decreto motivato da parte del Pubblico Ministero; ove questi non possa intervenire tempestivamente, la Polizia Giudiziaria può fare accertamenti urgenti su luoghi, cose e persone e disporre il sequestro. Il verbale è trasmesso entro quarantotto ore al P.M. del luogo dove il sequestro è stato eseguito e questi nelle quarantotto ore successive, convalida il sequestro con decreto motivato, se ne ricorrono i presupposti.

Per quanto attiene nello specifico al sequestro probatorio informatico, si deve rilevare *in primis* che l'art.19 della Convenzione sul *Cybercrime* chiarisce espressamente che il sequestro di strumenti informatici può riguardare indistintamente sia l'*hardware* (sistema informatico o supporto di memorizzazione), sia dati digitali in esso contenuti e presenti all'interno del territorio nazionale.

La Legge di Ratifica 48/2008 della Convenzione del Consiglio d'Europa sulla criminalità informatica ha modificato l'architettura normativa del sequestro originario, senza però snaturarlo.

Sono molteplici gli interventi riformatori in materia di sequestro probatorio.

II.4.1 **Il sequestro di corrispondenza.**

Si deve analizzare *in primis* la riformulazione dell'art. 254 c.p.p. relativo al *sequestro di corrispondenza,* all'interno del quale le novità apportate dalla L.48/2008 rilevano soprattutto sotto tre profili.

Il primo riguarda l'ampliamento del novero dei “soggetti”

destinatari del provvedimento di sequestro (cioè i fornitori di servizi postali, telegrafici e telematici), il cui elenco è tassativo.

La disposizione precedente, infatti, comprendeva solamente gli uffici postali e telegrafici e per tale ragione era diventata obsoleta.

Oggi, invece, molti di questi fornitori consentono agli utenti di creare un *account* di posta elettronica al fine di spedire e ricevere comunicazioni, continuando comunque ad offrire servizi tradizionali come raccomandate, posta ordinaria o telegrammi, ovviamente *online*.

Il secondo profilo rileva per l'ampliamento della tipologia della corrispondenza oggetto di acquisizione (ossia la corrispondenza telematica), grazie al quale è del tutto legittimo un provvedimento di sequestro dell'autorità giudiziaria su ogni comunicazione pertinente al reato inviata o ricevuta dall'indagato con strumenti elettronici.

È proprio nell'ambito dell'oggetto di acquisizione che in via generale (*ex art. 253 c.p.p)* va specificato, che nonostante la peculiarità della *res sequestranda,* è sempre necessaria la presenza del "rapporto di pertinenza" con il reato: deve cioè sussistere una stretta correlazione tra il bene da sottoporre a sequestro e le esigenze probatorie che il vincolo reale deve soddisfare.

Occorrerà dunque indicare con precisione per esempio la pagina web oggetto dell'indagine (all'interno di un sito) o ancora del particolare messaggio all'interno di un *forum*, il tutto per scongiurare ipotesi di sequestri "sovrabbondanti" e conseguentemente non idonei a soddisfare le esigenze

probatorie[81].

Infine, l'ultimo profilo è importante per l'inserimento del criterio della "non alterabilità" del reperto, che impone alla polizia giudiziaria incaricata del sequestro l'obbligo di garantire la genuina conservazione del materiale appreso.

II.4.2 **Il sequestro di dati informatici**

Il secondo intervento della L.48/2008 invece riguarda la creazione *ex novo* dell'art. 254-*bis* c.p.p., rubricato come "Sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni"[82].

La norma stabilisce che "l'autorità giudiziaria, quando dispone il sequestro, presso i fornitori di servizi informatici, telematici, o di telecomunicazioni, dei dati da questi detenuti, compresi quelli di traffico o di ubicazione, può stabilire, per esigenze legate alla regolare fornitura dei medesimi servizi, che la loro acquisizione avvenga mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità. In questo caso è, comunque, ordinato al fornitore di servizi di conservare e proteggere adeguatamente i dati originali".

Al di là del fatto che la prescrizione sia nata per proteggere le "esigenze legate alla fornitura dei servizi", è questo

81 F.CAJANI, *La rete internet e "dintorni", parte I- Aspetti tecnici ed investigazioni di base,* dal testo *Computer forensics e indagini digitali. Vol.II, Experta* 2011.

82 S.VENTURINI, *Sequestro probatorio e fornitori di servizi telematici,* dal testo *Internet provider* di L.Lùparia, Giuffrè 2009.

l'ulteriore segno di un *trend* in netta ascesa verso l'addossamento di incombenti investigativi a soggetti che assumono una posizione delicata, quali individui a rischio di concorso nel reato commesso dal cliente.

Occorre riflettere sul punto per trovare una soluzione di equilibrio, capace di contemperare le esigenze dell'accertamento con gli interessi difensivi di chi corre il pericolo di essere coinvolto nelle indagini cui è chiamato a collaborare, che a tutti gli effetti portatore di quel *privilege against self-incrimination:* benchè non formalmente sottoposto ad investigazione, rischia di far emergere una sua responsabilità proprio attraverso la dazione dei dati che gli vengono richiesti[83].

Il legislatore con la disposizione in commento, ha voluto ribadire *expressis verbis,* la generale sottoponibilità a tale mezzo istruttorio di tutti i dati informatici in possesso dei gestori ed ha altresì, indicato mediante l'utilizzo della locuzione "quando dispone" le precise modalità con cui tale operazione, invero già concepita dal nuovo testo dell'art 254 con riferimento alla corrispondenza, deve avvenire[84].

La norma in commento presenta poi una forte criticità, nella parte in cui fa riferimento al sequestro di "dati di traffico o di ubicazione", ove sembra sovrapporsi alla disciplina prevista dall' art. 132 del "*Codice della privacy"* (d.lgs. n. 196/2003).

Proprio per evitare che la disposizione entri in contrasto con la procedura garantita dall'art 132, oltre che dalle scansioni

---

83 L.LUPARIA, *I Profili Processuali,* in *Diritto Penale e Processo,* 2008, p.718

84 A.MACRILLO', *Le nuove disposizioni in tema di sequestro probatorio e di custodia ed assicurazione dei dati informatici,* in *Dir. Internet,*2008,p. 503

temporali di conservazione dei dati ivi contenute (*data retention*), è già stata proposta una interpretazione restrittiva, in realtà non priva di qualche forzatura ermeneutica.

In quest'ottica, l'art. 254-bis c.p.p disciplinerebbe il *quomodo,* ma non l'*an* del decreto di sequestro, ossia andrebbe solo a riempire di contenuti operativi l'art 254 c.p.p di cui costituirebbe una specificazione.

Sono state previste appunto delle precise indicazioni sulla necessità di assicurare l'acquisizione e la copia dei dati su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità.

Al contempo si è imposto al fornitore dei servizi di telefonia e di connessione internet una conservazione e protezione adeguata dei dati originali: da ciò si evince che la disposizione mira dunque ad evitare turbative alla regolare fornitura dei dati oggetto dell'interesse investigativo.

Sotto un profilo oggettivo, è opportuno precisare che con l'applicazione dell'art 254-*bis* c.p.p si possono acquisire con provvedimento di sequestro tutti i *file di log*[85] di navigazione sul *web* che rilevano ai fini dell'indagine.

Si garantisce in questo modo sia la regolare fornitura del sevizio di *Internet Service Provider* (che può continuare nonostante il provvedimento di sequestro), sia l'adempimento degli obblighi derivanti dalla normativa della *data retention (d.lgs. n. 109 del 2008 e art.132 del d.lgs.196 del 2003),* ovvero la cancellazione dei dati lì dove prevista per legge (ad

85*Log*: è un registro. Piccolo file o memoria ad alta velocità in grado di memorizzare dati, normalmente in formato testo, con lo scopo preciso di storicizzare gli eventi. Le registrazioni sono memorizzate sui file.

es. per il contenuto della comunicazione) e la conservazione dei dati stessi in maniera protetta fino al termine stabilito dall'art.132 del d.lgs.n.196/2003.

Quindi, a scanso di equivoci, è opportuno rammentare che il mezzo di ricerca della prova disciplinato dall'art. 254-*bis,* in ogni caso, ha ad oggetto dati informatici (detenuti dai *providers*) costituenti corpo del reato o cose pertinenti al medesimo e, per questa ragione, va tenuto distinto dall'attività "preventiva" disciplinata dall'art. 132 d.lgs. 196/2003 i cui risultati non sono utilizzabili nel procedimento penale, secondo quanto stabilito dall'art. 226 co. 5 d.lgs. 28 luglio 1989, n. 271.

Sulle "modalità di applicazione" dell'art 254-*bis* si pronuncia anche la Raccomandazione n.3 del 7 settembre 1999, formulata in sede Europea dal Gruppo di lavoro per la tutela delle persone, con riguardo al trattamento dei dati personali per la conservazione dei dati sulle comunicazioni da parte dei fornitori di servizi *internet* a fini giudiziari.

La normativa nazionale non sembra invece sufficientemente precisa sul punto.

L'art. 254-*bis* c.p.p., infatti, si limita a prevedere che l'autorità giudiziaria "possa" (e non debba) "stabilire per esigenze legate alla regolare fornitura dei medesimi servizi, che [l'acquisizione dei dati] avvenga mediante copia di essi su adeguato supporto...".

È proprio la previsione in via meramente possibilistica, e non della collaudata *best practice* della *bit stream image,* che dà origine a delle perplessità: in particolar modo suscita fondati dubbi di compatibilità della norma interna con l'ordito

normativo europeo.

Sicché una lettura costituzionalmente orientata e convenzionalmente conforme della norma, che tenga realmente conto di quelle "esigenze legate alla regolare fornitura dei medesimi servizi" e che rispetti gli *standard* raccomandati dalla citata fonte europea[86] suggerisce di seguire sempre la soluzione della clonazione del dato informatico secondo i protocolli scientifici.

In particolare, l'effettuazione della "copia" (auspicabilmente nel rispetto del principio del contraddittorio nella fase di estrazione del dato digitale) rappresenta il giusto contemperamento tra le esigenze di accertamento penale, di genuinità del dato informatico e di salvaguardia delle libertà costituzionalmente garantite.[87]

In base a tali considerazioni si può dedurre che con l'art 254-*bis* non sono state certamente definite le c.d *best practices* sulla miglior procedura da seguire per un corretto sequestro dei dati informatici, ma si è messo un punto fermo sotto il profilo della procedura da seguire in una materia delicata come quella dell' acquisizione "*in loco"*dei dati di traffico telefonico e telematico.[88]

---

86 Ossia: la base giuridica deve definire con precisione i limiti e le modalità di applicazione del provvedimento, i fini ai quali i dati possono essere trattati, il periodo di tempo durante il quale i dati possono essere mantenuti e le caratteristiche dell'accesso ai dati solo caso per caso e mai proattivamente o in via generale

87 S.VENTURINI, *Sequestro probatorio e fornitori di servizi telematici,* dal testo *Internet provider* di L.Lùparia, Giuffrè 2009.

88 S.ATERNO, *Richiesta di consegna e sequestro dei dati* digitali,dal testo *Computer Forensics e Indagini digitali* di S.Aterno, F.Cajani, G.Costabile, M.Mattiucci, G.Mazzarco, vol.1, Experta 2011.

II.4.3 **La tutela dei supporti posti sotto sequestro**

La legge di ratifica ha inoltre introdotto due ulteriori disposizioni relative alla *tutela* e alla *cura* da prestare ai supporti digitali posti sotto sequestro.

La prima è quella di cui all'art 259 comma 2 c.p.p. sulla "custodia delle cose sequestrate", laddove specifica che "*Quando la custodia riguarda dati, informazioni o programmi informatici, il custode è altresì avvertito dell'obbligo di impedirne l'alterazione o l'accesso da parte di terzi, salva, in quest'ultimo caso, diversa disposizione dell'autorità giudiziaria"*.

La seconda è la disposizione che ha modificato l'art 260 comma 2 c.p.p. sull'apposizione di sigilli e che ha introdotto la possibilità di ricorrere in casi particolari a sigilli di carattere informatico[89].

Si tratta in entrambi i casi di adeguamenti che nascono dal timore già più volte evidenziato, di vedere disperso o alterato il materiale informatico sequestrato.

Nel primo caso, l'intervento concerne appunto gli avvertimenti rivolti al custode individuato dall'autorità giudiziaria: nell'informatica forense e nella prassi applicativa delle tecniche di *computer forensics* questa metodologia prende il nome di "*Chain of custody"*(catena di custodia).

La Catena di custodia è un "documento" che deve accompagnare ogni fonte di prova acquisita all'interno dell'attività di *computer forensics,* ed è essenziale per la corretta attribuzione della responsabilità sulla fonte di prova stessa in ogni istante del suo ciclo di vita.

---

89 Ibidem

Essa deve essere affiancata al dato (o alla sorgente di dati), in modo da certificare l'originalità, l'integrità e le modalità con le quali è stato trattato[90].

La catena di custodia prevede un primo insieme di informazioni che permette di identificare univocamente il sistema da cui la *digital evidence* è stata estratta.

Le informazioni in questo senso riguarderanno: il "Tipo" di sistema contenente il dato (potrebbe essere un *desktop* ,un *server*, un palmare ecc.), la "Marca"del sistema che contiene la fonte di prova, il "Modello"del sistema, il "Numero seriale"del sistema ed infine il "Sistema operativo*"* presente sul sistema stesso (es. *Microsoft windows XP* o *Vista)*.

La catena di custodia prevede anche un secondo insieme di informazioni, che ha lo specifico obiettivo di mantenere traccia di tutti i soggetti che entrano in contatto con la fonte di prova: il termine catena di custodia deriva proprio dal fatto che è possibile, in qualsiasi momento, risalire al responsabile della custodia in un determinato istante temporale.

Le informazioni richieste a tal fine sono: la "Data"del momento in cui vi è stato il passaggio di custodia, e la prima data deve coincidere con la data sul documento che a sua volta dovrà coincidere con il momento d'acquisizione della *digital evidence*, e poi il "Cedente nominativo" e il "Ricevente nominativo", ossia rispettivamente il nome e cognome di colui che cede la *digital evidence* e nome e cognome di colui che la riceve.

Costituiscono un adeguamento dei precedenti contenuti

90 G.COSTABILE e G.MAZZARCO, *Identificazione, acquisizione ed analisi delle digital evidence: Approfondimenti tecnici,* dal testo, *Computer Forensics e Indagini digitali* di S.Aterno, F.Cajani, G.Costabile, M.Mattiucci, G.Mazzarco, vol.2, Experta 2011.

anche le modifiche apportate all'art. 260 commi 1 e 2 c.p.p.

La prima inserzione consente ora di apporre il "vincolo di sequestro", in relazione alla natura delle cose sequestrate, anche con mezzi elettronici: si "apre così la strada alla certificazione di conformità tra copia ed originale tramite la c.d. *Hash function*[91], vale a dire da un algoritmo matematico che partendo da un determinato *input* digitale di lunghezza arbitraria ottiene *output* di lunghezza fissa.

Il metodo di elaborazione comporta il cambiamento del codice di *output* in caso di mutamento dell' *input* originario.

Il procedimento risulta quindi un pesante e rigoroso sistema di controllo dell'errore[92]-

Al secondo comma, invece, dispone la possibilità di custodia degli originali sigillati anche in luoghi diversi dalla segreteria del P.M o della cancelleria del tribunale, conferendo così la facoltà di affidare in custodia all'indagato i dati sottoposti a vincolo nel supporto, permettendogli di utilizzare liberamente le parti non digitalmente vincolate.

Il sigillo digitale, disponibile *ex* art 260 c.p.p., è una criptazione dei dati originali acquisiti in copia, illeggibili ed immodificabili senza la chiave di decrittazione, che consente di affidarli in custodia senza rischi di inquinamento delle prove.

Le caratteristiche del sigillo digitale rendono l'avviso al custode di impedire l'alterazione o l'accesso dei dati ai terzi *ex* art 259 comma 2 c.p.p., superfluo nel caso di modificazione dei dati, necessario, invece, al solo fine di

---

91 L.LUPARIA, *I profili processuali,* in *Diritto Penale e Processo,* 2008.

92 L.CORDI', Commento *Modifiche al Titolo terzo del libro terzo del codice di procedura penale,* in *Legislazione Penale,2008.*

scongiurare la distruzione del supporto di memorizzazione .[93] Quest'ultima ipotesi però, oltre a configurare reato *ex* art. 388, comma 3, c.p., rubricato "Mancata esecuzione dolosa di un provvedimento del giudice", non influirebbe sulle indagini, in quanto gli inquirenti sarebbero già in possesso di una copia forense del supporto.

In conclusione, quindi, è facile comprendere come l'unico elemento che la prescrizione riflette è solo la costante preoccupazione per l'alterazione e dispersione dei dati, già più volte menzionata.

II.5 Le intercettazioni telematiche

Le comunicazioni telematiche hanno avuto negli ultimi tre decenni uno sviluppo esponenziale che ha contribuito a qualificare il nostro secolo come "il secolo dell'informazione", per la facilità con cui chiunque riesce a trovare, comunicare e diffondere informazioni in maniera economica ed immediata.

Nella vastità dei mezzi di comunicazione che ognuno di noi ha a disposizione ogni giorno, senza dubbio il più potente è quello della "comunicazione telematica", che avviene tramite un elaboratore elettronico (computer, telefono, lettore mp3 ecc.) fornito di una connessione a banda a larga che si può definire uno strumento di comunicazione "polifunzionale"[94].

---

93 F.NOVARIO, *Le prove informatiche,* dal testo *La prova penale,* a cura di P.Ferrua, E.Marzaduri, G.Spangher, Giappichelli-Torino, 2013.

94 E.CATANIA, *Profili essenziali delle intercettazioni telematiche. Dalla tutela costituzionale della segretezza ed inviolabilità di qualsiasi forma di comunicazione alla disciplina ex art. 266 c.p.p.*, dal sito www.diritto.it

Come già detto inizialmente, il crescente interesse mostrato dalle organizzazioni criminali verso strumenti di comunicazione che garantiscano rapidità ed efficacia dei collegamenti e sicurezza delle conversazioni, unitamente alle necessità di aggiornare le metodologie di indagine ai risultati del progresso tecnologico in campo informatico e telematico, hanno indotto il legislatore ad intervenire con la l. 547/ 1993, che ha introdotto nel nostro codice di procedura penale l'art. 266 *bis*, volto a regolare le "Intercettazioni di comunicazioni informatiche o telematiche".[95]

II.4.1 **La conformità al dettato costituzionale**

In una risalente sentenza della Corte Costituzionale[96] venne chiaramente affermato il principio secondo il quale le speciali garanzie predisposte dalla legge "*a tutela della segretezza e della libertà di comunicazione telefonica rispondono all'esigenza costituzionale per la quale l'inderogabile dovere di prevenire e reprimere i reati deve essere svolto nel più assoluto rispetto di particolari cautele dirette a tutelare un bene,* ***l'inviolabilità della segretezza e della libertà delle comunicazioni****, strettamente connesso alla protezione del nucleo essenziale della dignità umana e al pieno sviluppo della personalità delle formazioni sociali* (art.2 della Costituzione)".

In una pronuncia ancor più risalente[97], peraltro, il Giudice

95 F.Nevoli, *Intercettazioni informatiche e telematiche: ricorso ad impianti esterni ed obbligo motivazionale del pubblico ministero,* in *Arch.nuova proc.pen.2010 pag. 76.*

96 Corte Cost. Sent. n. 81 del 1993 in *www.giurcost.org*

97 Corte Cost. Sent. n. 75 del 1966 in *www.giurcost.org*

delle leggi, in termini decisamente più ampi ed astratti, evidenziava chiaramente come il contenuto dei diritti primari e fondamentali non potesse, considerarsi privo di limiti, sottolineando che l'art. 2 Cost., "*nell'affermare i diritti inviolabili dell'uomo e i doveri inderogabili di solidarietà politica, economica e sociale, non può escludere che a carico dei cittadini siano poste quelle restrizioni della sfera giuridica rese necessarie dalla tutela dell'ordine sociale",* anche se i diritti connotati dalla inviolabilità *"essendo intangibili nel loro contenuto di valore, possono essere unicamente disciplinati da leggi generali che possono limitarli soltanto al fine di realizzare altri interessi costituzionali altrettanto fondamentali e* generali"[98].

Dette restrizioni – afferma ancora la Corte[99] - sono necessarie poiché "*i diritti primari e fondamentali dell'uomo diverrebbero illusori per tutti, se ciascuno potesse esercitarli fuori dell'ambito della legge, della civile regolamentazione, del costume corrente, per cui tali diritti devono venir contemperati con le esigenze di una tollerabile convivenza*" e la regola da seguire affinché tali limiti siano ammissibili è quella della "*necessarietà e ragionevolezza della limitazione*[100]".

In questa prospettiva, rispetto alla libertà e alla segretezza delle comunicazioni garantite dalla Carta Costituzionale**,** la Corte ha sottolineato che "*la stretta attinenza di tale diritto al nucleo essenziale dei valori di personalità – che inducono a qualificarlo come parte necessaria di quello spazio vitale*

98 Corte Cost. Sent. n. 235 del 1988 in *www.giurcost.org*
99 Corte Cost. Sent. n. 168 del 1971 in *ww.giurcost.org*
100Corte Cost. Sent. n. 141 del 1996 in *www.giurcost.org*

che circonda la persona e senza il quale questa non può esistere e svilupparsi in armonia con i postulati della dignità umana – comporta una duplice caratterizzazione della sua inviolabilità.

In base all'art. 2 della Costituzione, *il diritto a una comunicazione libera e segreta è inviolabile, nel senso generale che il suo contenuto essenziale non può essere oggetto di revisione costituzionale, in quanto incorpora un valore della personalità avente un carattere fondante rispetto al sistema democratico voluto dal costituente.*

In base all'art. 15 della Costituzione, d'altra parte, *lo stesso diritto è inviolabile nel senso che il suo contenuto di valore non può subire restrizioni o limitazioni da alcuno dei poteri costituiti se non in ragione dell'inderogabile soddisfacimento di un interesse pubblico primario costituzionalmente rilevante, sempreché, l'intervento limitativo posto in essere sia strettamente necessario alla tutela di quell'interesse e sia rispettata la duplice garanzia che la disciplina prevista risponda ai requisiti propri della riserva assoluta di legge e la misura limitativa sia disposta con atto motivato della autorità giudiziaria*[101].

Questa, è quindi, la cornice Costituzionale di riferimento all'interno della quale collocare il complessivo sistema di garanzie e tutele in relazione al mezzo delle intercettazioni sul quale si concentrerà il prosieguo della trattazione. L'inevitabile estensione legislativa del concetto di comunicazione a tutte le forme di trasmissione di dati in forma digitale, pertanto, determina l'operatività anche per le

101Corte Cost. Sent. n. 366 del 1991 in *www.giurcost.org*

stesse della tutela prevista dall'art. 15 della Costituzione che, come indicato *supra*, definisce "inviolabili" "la libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione" e ne consente la limitazione "soltanto per atto motivato della A.G. con le garanzie stabilite dalla legge".

In maniera sicuramente condivisibile, il legislatore ordinario ha ritenuto non assimilabili – e quindi non sovrapponibili ai fini della specifica disciplina normativa - le due espressioni *"con le garanzie stabilite dalla legge",* adoperata dall'art. 15 Cost. e *"nei soli casi e modi stabiliti dalla legge",* di cui all'art 13 Cost. (cui fra l'altro rinvia l'art. 14 Cost.).

Questa impostazione è stata peraltro condivisa ed avallata dalla Corte Costituzionale che, in una famosa sentenza ha sottolineato[102] come il difficile contemperamento tra tutela della libertà e segretezza delle comunicazioni, da un lato, ed esigenza di prevenire e reprimere i reati, dall'altro, non può non trovare esplicazione nella puntuale e dettagliata disciplina che il legislatore deve predisporre al fine di regolamentare le concrete modalità (tecniche ed operative) attraverso le quali i servizi di intercettazione debbono essere predisposti, assicurando stabilmente alla A.G. la possibilità di effettuare una penetrante e pronunciata attività di controllo (non soltanto di matrice giuridica, bensì, come si vedrà in seguito, anche sugli apparati e le materiali tecnologie di captazione utilizzate nell'ambito del singolo procedimento).

102Corte Cost. Sent. n. 34 del 1973 in *www.giurcost.org*

II.4.2 **L'ambito oggettivo di applicazione**

Come si è detto *supra*, l'art. 15 della Costituzione, dopo avere proclamato inviolabili la libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione, ne consente tuttavia la limitazione, purché, con atto motivato dell'autorità giudiziaria e con le garanzie stabilite dalla legge. In ottemperanza a questo preciso dettato costituzionale, il legislatore, pur nella consapevolezza delle notevoli potenzialità delle intercettazioni, ha ritenuto di dover circoscrivere entro precisi limiti il relativo potere delle autorità inquirenti, stabilendo in maniera tassativa, quali sono le fattispecie di reato per le quali è consentito il ricorso a questo mezzo di ricerca della prova (delitti puniti con l'ergastolo o la reclusione superiore nel massimo a cinque anni; delitti contro la Pubblica Amministrazione puniti con pena non inferiore a cinque anni; delitti in materia di stupefacenti, armi ed esplosivi; delitti di contrabbando, ingiuria, minaccia, usura, abusiva attività finanziaria, abuso di informazioni privilegiate, manipolazione del mercato, pornografia minorile, anche cd. "virtuale").

Ancor prima della emanazione della legge n.547 si faceva rientrare il concetto di intercettazione telematica, nel novero della disciplina delle intercettazioni di comunicazioni ex art. 266 co. 1 (ove appunto si parla di "altre forme di telecomunicazioni"), ma è altrettanto vero che detta sussunzione, dava luogo ad una equiparazione che appare immediatamente priva di fondamento qualora si proceda ad una analisi delle informazioni trasmesse via telefono,

contrapponendole a quelle trasmesse via *computer*.

Le intercettazioni telefoniche consentono di inserirsi in una trasmissione "fonica" passante per una linea dedicata o commutata: sono, quindi, in grado di accertare che sia in corso una comunicazione, che ci sia uno scambio di impulsi tra *modem*.

Non sono in grado però di decifrarne il contenuto.

Ed è proprio per l'attività di decifrazione delle informazioni trasferite via *modem* che è stata predisposta l'intercettazione informatica: i suoni o gli impulsi trasmessi via computer vengono infatti intercettati e decifrati in informazioni interpretabili da un altro *computer* (a disposizione degli inquirenti) che le renderà comprensibili all'uomo.

La disciplina delle nuove tipologie di intercettazioni venne per molti aspetti modellata su quella delle intercettazioni ordinarie, prevedendo però al contempo anche una serie di aspetti normativi ed operativi del tutto autonomi.

Nello specifico le intercettazioni informatiche e telematiche sono state introdotte con la l. 547/1993 e corrispondono all'art. 266 *bis*.

L'art. 266 *bis* c.p.p., appunto, prevede che: "N*ei procedimenti relativi ai reati indicati nell'articolo 266 nonché a quelli commessi mediante l'impiego di tecnologie informatiche o telematiche, è consentita l'intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici"*.

L'interpretazione di tale disposizione ha suscitato non pochi dubbi.

Una parte della dottrina[103], sulla base del presupposto che la tassatività delle ipotesi in cui è consentita la violazione della segretezza delle comunicazioni non può non valere per tutte le "categorie" di intercettazioni, riteneva la scelta del legislatore chiaramente orientata nel senso di "limitare" l'uso delle intercettazioni informatiche all'accertamento di una determinata categoria di reati.

Questa impostazione fondava la sua *ratio* nella considerazione che, per assicurare alla giustizia i colpevoli di particolari tipi di reato - realizzabili soltanto grazie all'uso di strumenti informatici o telematici – fosse inevitabile violare la privacy delle comunicazioni che avvengono via *computer*, ma riteneva anche non occorresse a tal fine comprimere la libertà delle comunicazioni che vengono realizzate via telefono o altrimenti.

La differenziazione operata dal legislatore sembrerebbe in quest'ottica, legittimata dall'intento di circoscrivere al massimo le interferenze nelle comunicazioni altrui.

D'altra parte se si rifiutasse l'interpretazione restrittiva, si dovrebbe ammettere la legittimità dell'intercettazione informatica come mezzo di ricerca della prova per quei reati non compresi nell'elenco dell'art. 266 c.p.p. - per i quali, se non fossero realizzati con particolari moderne tecnologie, nessun altro mezzo di intercettazione sarebbe ammissibile.

Si potrebbe ravvisare, allora, una disparità di trattamento (e dunque una violazione dell'art. 3 della Costituzione) tra i diversi imputati di uno stesso reato commesso con modalità

---

103 S.ATERNO, *Acquisizione dati traffico ed intercettazioni telematiche,* in *Computer forensics e Indagini digitali. Manuale tecnico-giuridico e casi pratici.* Experta, 2011, p. 344

tecniche differenti, le une legittimanti e le altre no l'intercettazione informatica: a parità di imputazione, infatti, l'inviolabilità delle comunicazioni sarebbe garantita solo se il reato fosse commesso senza l'uso di strumenti informatici[104].

Tuttavia, un'interpretazione estensiva[105], ribatteva che né la lettera né lo spirito della legge n. 547 del 1993 legittimavano un'interpretazione restrittiva; secondo tale impostazione le intercettazioni di cui all'art. 266 bis c.p.p. dovevano essere ammesse sia per i reati informatici cc.dd. propri (quelli cioè in cui l'uso del *computer* è elemento costitutivo) sia per i *reati informatici impropri* (in cui l'uso del *computer* integra solo una delle modalità della condotta).

La Corte di Cassazione a Sezione Unite[106] è intervenuta a risolvere la questione affermando che la novità dell'art 266-*bis* risiede proprio "nell'aver esteso l'ambito di ammissibilità delle intercettazioni ai procedimenti aventi ad oggetto i *computer-crimes,* ma anche nell'aver consentito l'intercettazione dei flussi di dati presenti nei singoli sistemi.

Quanto, poi, alla pretesa disparità di trattamento fra imputati di uno stesso reato commesso con modalità tecniche differenti, paventata dai sostenitori dell'opposta tesi, essa è pienamente giustificata dalla maggiore pericolosità di cui è sintomo l'uso di un differente strumento che caratterizza la condotta[107].

L'opzione legislativa è stata pertanto ispirata dalla necessità di ampliare, *in subiecta materia,* le ipotesi di esperibilità del

104L. UGOCCIONI, *Criminalità informatica,* in *L.P.* 1996, p. 141

105C.PARODI, *La disciplina delle intercettazioni telematiche,* in *Dir. pen.e proc.,* 2003, p. 889

106Cass.Sez.Un., 24 settembre 1998, n.21, in *Giust. Pen.,* 614

107A.CAMON, *Le intercettazioni nel processo penale,* Giuffrè, 1993, p. 12 ss.

mezzo di ricerca della prova in oggetto, dovendosi prendere atto della impossibilità di controllare e reprimere seriamente determinate forme di criminalità senza ricorrere a siffatta, peculiare forma di intercettazione delle comunicazioni.

A tal fine, il legislatore ha dovuto garantire un ambito di operatività della disciplina in esame, potenzialmente espandibile parallelamente al progresso scientifico e tecnologico.

Alla luce delle considerazioni sin qui menzionate, è, allora, possibile tracciare il seguente quadro: a) quando le indagini hanno ad oggetto uno dei reati indicati dall'art. 266 c.p.p., sia o meno commesso con l'impiego di tecnologia informatica, l'autorità inquirente può ricorrere sia alle intercettazioni comuni sia a quelle informatiche; b) quando le indagini hanno ad oggetto reati diversi da quelli contenuti nell'elenco di cui all'art. 266 c.p.p., sono possibili solo le intercettazioni informatiche, sempre che i reati in questione siano stati commessi mediante l'uso di tecnologie informatiche o telematiche anche se gli stessi non sono ricompresi nel novero dei *cybercrimes.*

In ragione di quanto appena affermato, per determinati illeciti informatici di gravità poco più che bagatellare sarà - ove ricorrano tutti i presupposti normativi - concedibile l’intercettazione telematica, ma non quella telefonica.

Si tratta di una circostanza non priva di rilevo pratico, specie per l’attuale prassi investigativa, giacché alcune strumentazioni utilizzate per acquisire il flusso telematico possono contemporaneamente intercettare il traffico telefonico, sollevando forti dubbi di invalidità e quindi

esponendo alla sanzione di inutilizzabilità (*ex* art. 271 c.p.p.) il complesso dei risultati acquisiti.

Uniforme appare, invece, il giudizio sul significato da attribuire alle espressioni "sistema informatico"e "sistema telematico".

Sebbene la Convenzione sul *Cybercrime* non distingua nettamente tra sistema informatico e telematico, secondo la dottrina[108] è ormai consolidata la definizione di "sistema informatico" come un complesso costituito da più elaboratori elettronici collegati tra loro per scambiare dati, ma può essere costituito anche da un solo elaboratore, purchè collegato ad altri strumenti informatici, detti periferiche, per la realizzazione specifica di una funzione o applicazione.

Il sistema telematico è invece definito come un sistema in cui gli elaboratori non sono in permanenza collegati tra loro da un cavo di connessione, ma utilizzano cavi telefonici, modulatori di toni e satelliti artificiali.

In breve, il *discrimen* tra i due è il metodo utilizzato per la trasmissione dei dati a distanza: i sistemi informatici sono collegati direttamente attraverso il cavo, i sistemi telematici attraverso le linee telefoniche.

---

108 S.ATERNO, *Acquisizione dati traffico ed intercettazioni telematiche,* in *Computer forensics e Indagini digitali. Manuale tecnico-giuridico e casi pratici.* Experta, 2011, p. 348

II.4.3 **I presupposti procedurali: gravi indizi di reato e assoluta indispensabilità**

In merito ai presupposti procedurali per l'avvio delle intercettazioni telematiche, la disciplina applicabile è quella di cui all'art. 267 c.p.p. con la tipica richiesta da parte del P.M. al giudice per le indagini preliminari dell'autorizzazione a disporre le intercettazioni.

Il Giudice quindi valuterà l'esistenza dei presupposti previsti da tale articolo in generale per le intercettazioni, ossia "i gravi indizi di reato" e "l'assoluta indispensabilità" per la prosecuzione delle indagini.

Quanto ai primi, essi attengono alla mera esistenza del reato e non alla colpevolezza di un determinato soggetto; per procedere ad intercettazione non è pertanto necessario che i detti indizi siano a carico dei soggetti le cui comunicazioni debbano essere, ai fini investigativi, intercettate[109].

Quanto al secondo presupposto normativo appunto, l'indispensabilità, è da considerarsi non alternativo bensì giustapposto ai gravi indizi di reato.

Va ancora precisato che il requisito dei gravi indizi di reato deve essere inteso non in senso probatorio (ossia come valutazione del fondamento dell'accusa), bensì come vaglio di particolare serietà delle ipotesi delittuose configurate, che non devono risultare meramente ipotetiche, con la conseguenza che è da ritenere legittimo il decreto di intercettazione telefonica disposta nei confronti di un soggetto che non sia iscritto nel registro degli indagati[110].

---

109 Cass. Sez. VI, 18 giugno 1999, n. 9428, Patricelli; Sez. V, 7 febbraio 2003, n. 38413, Alvaro e altri in *www.cortedicassazione.it*

110 SS.UU. 17 novembre 2004, n. 45189, Esposito, in *Cass. pen.,* 2005,

Alla stregua dell'orientamento prevalente in giurisprudenza, il requisito della indispensabilità delle intercettazioni (che, ai sensi dall'art. 267 comma 1, deve essere assoluta) ai fini della prosecuzione delle indagini, può essere valutato esclusivamente dal giudice di merito, la cui decisione può essere censurata, in sede di legittimità, solo sotto il profilo della manifesta illogicità della motivazione[111].

E' noto che il legislatore del 1991[112] abbia attenuato i presupposti legittimanti il ricorso allo strumento delle intercettazioni per indagini su "delitti di criminalità organizzata o di minaccia col mezzo del telefono", prevedendo che l'intercettazione non sia "indispensabile", ma semplicemente "*necessaria*" per le anzidette indagini e richiedendo al contempo indizi (rispetto a detti reati) non "gravi", ma solo "*sufficienti*".

Procedendo nell'analisi dell'art. 267 co. 2 c.p.p., esso prevede "nei casi d'urgenza", quando vi è fondato motivo di ritenere che dal ritardo nell'esecuzione dell'intercettazione possa derivare grave pregiudizio alle indagini, "il Pubblico Ministero dispone l'intercettazione con decreto motivato, che va comunicato immediatamente e comunque non oltre le ventiquattro ore al Giudice per le indagini preliminari il quale, entro quarantotto ore dal provvedimento, decide sulla convalida con decreto motivato".

In caso di mancata convalida nel termine stabilito

---

p.343

111 Sez. VI, 25 settembre 2003, n. 49119, Scremin, in *Cass. pen,* 2005. p. 3926

112 Art. 13 d.l. 13 maggio 1991 n. 152 conv. in l. 12 luglio 1991, n. 203, successivamente modificato dall'art. 3-bis d.l. 8 giugno 1992, n. 133 conv. in l. 7 agosto 1992, n. 356 e da ultimo dall'art. 23 l. 1° marzo 2001, n. 63

“l'intercettazione non può essere proseguita e i risultati di essa non possono essere utilizzati”.

In materia di *cybercrime* il minimo comune denominatore solitamente è costituito dalla necessità di agire con particolare celerità nell'attività di ricerca della prova, soprattutto considerando l'estrema e naturale volatilità delle tracce informatiche.

Pertanto come avviene in taluni casi per le intercettazioni telefoniche, anche le intercettazioni telematiche possono essere disposte “in via d'urgenza” direttamente dal P.M. con decreto al quale poi dovrà seguire l'eventuale convalida del Giudice.

Entro cinque giorni dalla conclusione delle operazioni e non oltre la chiusura delle indagini, ai difensori delle parti è riconosciuta la facoltà di esaminare gli atti, ascoltare le registrazioni ovvero prendere cognizione dei flussi di comunicazione telematiche.

Le modalità esecutive delle operazioni di intercettazione, sono invece disciplinate dall'art. 268 c.p.p, il quale statuisce al comma 3° che “le operazioni possono essere compiute esclusivamente per mezzo degli impianti installati nella procura della Repubblica tuttavia, quando tali impianti risultino insufficienti o inidonei ed esistano eccezionali ragioni d' urgenza, il P.M. può disporre con provvedimento motivato il compimento delle operazioni mediante impianti di pubblico servizio o in dotazione alla Polizia giudiziaria”.

Tale previsione è particolarmente rigorosa: la sua violazione infatti è sanzionata *ex* art. 271 c.p.p. con *l'inutilizzabilità* dei risultati delle intercettazioni.

II.4.4 **Intercettazioni mediante impianti appartenenti a privati**

La l. 547/1993, nel tentativo di adattare la disciplina codicistica alla peculiare figura delle intercettazioni informatiche o telematiche, ha inserito nell'art. 268 c.p.p., il comma 3-*bis*.

Questo prevede che "quando si procede a intercettazione di comunicazioni informatiche o telematiche, il Pubblico Ministero, possa disporre che le operazioni siano compiute anche mediante impianti appartenenti a privati".

Si tratta di un aspetto delicato e che pone non pochi problemi di natura interpretativa[113].

Prima di tutto si tratta di una previsione che determina una possibilità espressa di deroga alla rigorosa disciplina prevista dall'art. 268: il comma 3-*bis* infatti non prevede la facoltà per il P.M. di fornire motivazione al suo provvedimento e, soprattutto, non prevede nessun specifico presupposto per l'esecuzione delle operazioni con impianti diversi da quelli dell'Ufficio di Procura.

Sostanzialmente, al PM è lasciata assoluta discrezionalità nell'uso degli impianti appartenenti a privati, trattandosi di strumenti ad alto "tasso"di tecnologia, di cui le Procure e gli Uffici di Polizia Giudiziaria non sono effettivamente dotati.

La previsione di un comma autonomo rispetto al comma 3 dell'art. 268 c.p.p., consente quindi, in ossequio a criteri

113 S.ATERNO, *Acquisizione dati traffico ed intercettazioni telematiche,* in *Computer forensics e Indagini digitali. Manuale tecnico-giuridico e casi pratici.* Experta 2011, p. 357

eminentemente pratici, di ritenere che la facoltà ivi prevista debba ritenersi del tutto autonoma e svincolata dai criteri stabiliti per l'utilizzo in generale di impianti di pubblica utilità, avendo verosimilmente il legislatore preso atto della cronica sottodotazione strutturale delle sedi giudiziarie, oltre che della totale "assenza", al momento di entrata in vigore della legge, di idonee apparecchiature presso gli uffici normalmente deputati alle attività in oggetto.

Il ricorso agli impianti dei privati, pertanto, non costituisce affatto un'eccezione, ma semmai la regola per l'esecuzione di intercettazioni telematiche od informatiche.

Per il disposto generale dell'art. 267,3° co., c.p.p., pertanto, al PM basterà indicare nel decreto "dispositivo" delle intercettazioni le "modalità" di esecuzione, senza che possa derivare alcuna sanzione processuale per il caso che ometta di motivarne la scelta.

Tuttavia, una parte della dottrina[114] ritiene che la disposizione di cui al comma 3-*bis* costituisca una mera prosecuzione del comma 3 dell'art. 268 e che le due norme si pongano l'una rispetto all'altra in rapporto di *species* a *genus*, sussistendo fra esse un collegamento non soltanto lessicale, ma anche logico.

Questa interpretazione troverebbe conferma nell'uso della congiunzione "anche" nel comma 3-*bis*, che può essere agevolmente inteso come diretto - fermi i presupposti previsti dal comma 3 - ad inserire un'ulteriore alternativa dinanzi ad una situazione di impossibilità a utilizzare gli

114 F.NEVOLI, *Intercettazioni informatiche e telematiche: ricorso ad impianti esterni ed obbligo motivazionale del P.M., Arch. Nuova proc. Pen.,* 2010, p. 76

apparati della Procura.

In questo senso, l'unica lettura consentita dei due commi in argomento, sarebbe quella "unitaria" che consentirebbe, fra l'altro, il necessario coordinamento del nuovo comma con le norme concernenti i divieti di utilizzazione.

Di tal guisa, dalla violazione dei limiti posti all'utilizzazione di impianti privati per le intercettazioni telematiche ed informatiche deriverebbero le consequenziali sanzioni dell'inutilizzabilità dei risultati delle captazioni, e ciò benché l'art. 271 c.p.p. (in tema, appunto, di inutilizzabilità) non contenga alcun riferimento al comma *3-bis*.

In questo senso si è espressa la Corte di Cassazione[115] che, in ossequio ai principi formulati in tema di intercettazioni dalla Corte Costituzionale,[116] asserisce che il legislatore nel regolamentare all'art.271 c.p.p. la sanzione processuale della inutilizzabilità del contenuto delle intercettazioni (norma, fra l'altro, entrata in vigore prima che venisse introdotto il comma *3-bis*) ha avuto presente non soltanto le captazioni di comunicazioni telefoniche, ma anche quelle di ogni tipo di comunicazione, quali che siano le peculiari modalità di svolgimento.

Nel momento in cui le operazioni di intercettazione si concludono, si apre il procedimento di ammissione della prova[117].

I verbali redatti e le registrazioni eseguite nel corso delle intercettazioni, immediatamente trasmesse al p.m., vanno depositati in segreteria, insieme ai provvedimenti (di

115 Cass. Sez. I Sent. 28 settembre 1999 n.5239
116 Corte Cost. 4 aprile 1973 n. 34
117 A. NAPPI, *Sull'abuso delle intercettazioni,* in *Cass. pen.,*2009, p.472

autorizzazione ed eventualmente di proroga) concernenti l'intercettazione, entro cinque giorni dalla conclusione delle operazioni, salvo che il giudice autorizzi il ritardo del deposito non oltre la chiusura delle indagini preliminari, quando potrebbe derivarne grave pregiudizio per le investigazioni (art. 268 commi 4 e 5 c.p.p.).

I difensori delle persone sottoposte alle indagini hanno entro un termine fissato dal p.m., la facoltà di esaminare gli atti e ascoltare le registrazioni, ovvero, prendere cognizione dei flussi di comunicazione.

Scaduto il termine, il giudice dispone l'acquisizione delle conversazioni o dei flussi di comunicazioni informatiche o telematiche indicati dalle parti, che non appaiano manifestamente irrilevanti, procedendo anche di ufficio allo stralcio delle registrazioni e dei verbali di cui è vietata l'utilizzazione.

È ovvio, che la selezione delle comunicazioni rilevanti debba considerarsi momento fondamentale dato che, talvolta, riuscire ad "includere" o "escludere" parti delle comunicazioni può essere determinante per gli esiti della vicenda giudiziaria[118].

In ultimo il legislatore con l'art. 13 della l. 547/1993, aveva inoltre previsto la possibilità di disporre intercettazioni telematiche anche in relazione alle cosiddette "intercettazioni preventive" disciplinate dalla l. 356/1992.

La *ratio* della modifica era quella di aumentare gli strumenti tecnologici per cercare di migliorare la lotta alla criminalità organizzata e ad alcuni tipi di delitti di particolare gravità e

118 A. NAPPI, *Sull'abuso delle intercettazioni,* in *Cass. pen.,*2009, p.473

sono consentite esclusivamente per i delitti indicati nell'art. 51 comma 3-*bis* c.p.p.

Ancora un aspetto da esaminare è quello dell'analisi dei protocolli che vengono applicati all'intercettazione telematica, i quali si articolano su taluni caratteristici (e ricorrenti) passaggi tecnici.

Occorre infatti decriptare un segnale digitale e memorizzarlo su un apposito supporto; ma, ancor prima, è necessario individuare il *client* cui riferire la comunicazione, e poi individuare il soggetto (persona fisica) che abbia avuto in uso lo strumento elettronico e che abbia effettuato la connessione durante la quale è stato consumato l'illecito.

Di certo - stante il principio della responsabilità personale - non ci si potrà accontentare di identificare il numero di telefono chiamante o chiamato, ma occorrerà approfondire le indagini con accertamenti documentali (contratti, moduli di fatturazione,ecc.) ovvero storici (analisi delle ulteriori chiamate effettuate) nel tentativo di appurare la concreta disponibilità dell'utenza e del mezzo informatico ad un soggetto fisico ben individuato.

II.4.5 **L'analisi dei dati oggetto di intercettazione**

L'analisi dei dati intercettati si articola tipicamente secondo il seguente modulo:

a) ogni *server* di accesso alla rete, al momento della connessione ("*log-in*") crea un file di log dell'utente, contenente le seguenti informazioni-base:

- *user name*;
- data, ora e secondi dell'inizio della connessione (*log-in*) e del termine della connessione (*log-out*);
- IP dinamico assegnato e *caller* ID, cioè numero del telefono chiamante;

b) qualora l'utente si colleghi ad un server di posta elettronica (un server cioè di 2° livello, differente dal server fornitore di connettività – c.d. *provider*), esso annoterà a sua volta l'accesso, registrando ancora:

- *user name*;
- data, ora e secondi del login e del *logout* sincronizzati su "*time server*"[119]
- IP dinamico

Inoltre, parametri altrettanto oggettivi quali le coordinate fornite dai c.d. *Mac Address*[120] , le interfacce di rete *wireless* degli *Access Point* (difficilmente modificabili), possono essere presi in considerazione, in virtù della loro affidabilità, al fine di accertare in dibattimento il dipanarsi di operazioni considerate volatili.

Sulla base degli elementi sopra indicati sarà quindi possibile cercare di risalire all'effettivo utilizzatore delle linee telefoniche utilizzate per la connessione (*caller* ID chiamanti) e quindi ai singoli utenti, incrociando le

---

119 Computer presenti nella rete Internet il cui compito consiste nel sincronizzare gli orologi dei computer all'interno di una rete di commutazione di pacchetto (Internet) utilizzando il protocollo NTP :Il *Network Time Protocol.*

120 In informatica e telecomunicazioni l'indirizzo MAC (in inglese MAC address, dove MAC sta per Media Access Control), detto anche indirizzo fisico, indirizzo ethernet o indirizzo LAN, è un codice di 48 bit (6byte)assegnato in modo univoco dal produttore ad ogni scheda di rete ethernet prodotta al mondo (peraltro esistono software in grado di camuffare detto codice).

informazioni derivanti dai dati costituiti dai *file di log*, dai dati di registrazione presso il *provider*, da quelli risultanti dal tabulato telefonico dell'utenza dalla quale risulta effettuato il collegamento al provider, nonché dagli altri ulteriori parametri di cui si è detto.

In quest'ottica, peraltro, le problematiche con le quali ci si deve misurare sono quelle connesse all'impiego di *Internet* in combinazione con i vari servizi di anonimizzazione esistenti (*proxy, anonymizer* a pagamento, algoritmi di crittazione ecc. ecc.), all'impiego di SIM o USIM estere o rubate/trafugate, ovvero con la possibilità di sfruttare la connettività offerta da c.d. *Internet Cafè,* accorgimenti cioè che consentono ad operatori (anche non molto esperti) di assicurarsi un notevole livello di anonimato.

Dal punto di vista tecnico, la captazione dei flussi sottoposti ad intercettazione può essere effettuata: deviando i medesimi flussi sul sistema intercettante, che provvederà a memorizzarli e, quindi, a ritrasmetterli al destinatario; ovvero inserendo sul *computer* intercettato un "registro degli eventi" in grado di memorizzare gli inserimenti dei dati di interesse investigativo; oppure ancora - nel caso di intercettazioni telematiche - registrando i flussi dopo aver provveduto ad attivare un'apposita linea telefonica (RES) fornita di *modem* per ricevere le comunicazioni oggetto delle indagini.

Le operazioni di intercettazione potranno inoltre avvenire o direttamente sulla linea telefonica dell'utente, interponendosi tra utente e *provider*, ovvero sfruttando la stessa rete del *provider.*

In atto le tecnologie d'intercettazione più diffuse sono

costituite dagli analizzatori di protocollo.

Di *protocol analyzer* se ne trovano numerosi disponibili gratuitamente (*open source*) anche sul *web*.

Essi sono installati presso i *provider* e sono in grado di intercettare tutto il flusso dati relativo ad una determinata linea di comunicazione.

Su tale flusso dati si possono anche impostare taluni filtri al fine di selezionare i dati da catturare in ragione di specifiche esigenze investigative.

L'utente di un servizio internet, come noto, vi può accedere da diversi punti e con diverse tipologie di collegamento.

Se è palese che il soggetto cambia continuamente via di collegamento, magari perché in movimento o perché avveduto della possibilità di essere controllato, bisogna impiegare una metodologia di intercettazione che operi contemporaneamente su più canali (audio/video/dati).

A tal fine, frequentemente impiegato nelle indagini informatiche è il cd. "*telemonitor*": si tratta di un sistema che intercetta il flusso dati in partenza ed in arrivo da e verso l'utente, che offre la possibilità di ricostruire in modo intelligibile i segnali analogici della comunicazione tra i *modem*, e che si colloca sulla linea telefonica dell'utente "a metà strada" tra l'utente stesso ed il provider.

Accade però che tale sistema venga eluso tutte le volte in cui l'indagato utilizzi per la connessione una linea telefonica diversa da quella consueta.

In questo caso, gli stessi dovranno essere inseriti su più linee e punti come osservatori.

Alla fine il G.I.P. dispone la trascrizione integrale delle

registrazioni ovvero la stampa in forma intellegibile delle informazioni contenute nei flussi di comunicazione informatiche o telematiche da acquisire osservando i modi e le garanzie previste dall'art. 268 comma 7.

Tale precisione sulla forma intellegibile della stampa, si è resa necessaria alla luce della natura del dato informatico, altrimenti comprensibile solo per gli esperti in materia.

L'ultima considerazione da fare è che in realtà la portata innovativa del 266 *bis* è meno rilevante di quanto *prima facie* appaia.

Difatti l'art. 266 c.p.p., già consentiva "l'intercettazione di conversazioni o comunicazioni telefoniche o di altre forme di telecomunicazione", non v'è dubbio pertanto che tutte le comunicazioni che avvengono avvalendosi del sistema telefonico, nelle sue forme più disparate, risultino comprese nel concetto di comunicazioni telefoniche o telecomunicazioni.

Di conseguenza in maniera specifica solo le "intercettazioni informatiche" aventi per oggetto più *computer* che interagiscono tra loro, senza l'uso del mezzo telefonico, come nel caso di elaboratori collegati tra loro da una rete *LAN (Local Area Network)* possono ritenersi introdotti *ex novo* nel nostro ordinamento a seguito della novella del 1993.[121]

121F.NEVOLI, *Intercettazioni informatiche e telematiche: ricorso ad impianti esterni ed obbligo motivazionale del pubblico ministero,* in *Arch.nuova proc.pen.* 2010 *Pag. 77*

II.5 L'alibi informatico

L'analisi degli elaboratori elettronici e più in generale degli apparati di comunicazione digitale può risultare fondamentale nel corso dell'attività investigativa per molteplici motivazioni.

Tra di esse rilevano, ai fini del presente lavoro, quelle in cui le tracce informatiche possono essere utilizzate per dimostrare sia la colpevolezza sia la totale estraneità dell'indiziato rispetto alle accuse formulate nei suoi confronti.[122]

Non è raro che le suddette tracce oltre ad essere ricercate dagli organi inquirenti, siano fornite appositamente dalla difesa dell'indagato o direttamente da quest'ultimo, con l'obiettivo di ricostruire un c.d. "Alibi" capace di smentire i fatti di reato ascrittigli.

Bisogna precisare però che l'individuazione e la ricostruzione di un alibi non sono scelte difensive necessarie, visto l'assodato criterio secondo cui "dalla sua assenza non può farsi discendere la colpevolezza dell'imputato, in mancanza di elementi di prova che ne dimostrino la responsabilità al di là di ogni ragionevole dubbio".

Il termine alibi non trova definizione all'interno del nostro codice e nemmeno ne viene fatta menzione specifica tra i mezzi di prova codificati.

Si tratta di un avverbio di lingua latina che significa

122 F. CAJANI e S. ATERNO, *Aspetti giuridici comuni delle indagini informatiche,* dal testo *Computer forensics e indagini digitali. Manuale tecnico-giuridico e casi pratici.* Experta 2011.

"altrove": rappresenta infatti "l'altro luogo" in cui si trovava l'indiziato nello stesso arco temporale in cui "altrove" veniva commesso un delitto. Pertanto, esso contiene "un forte substrato semantico di tipo evocativo ed emotivo che riecheggia, anche nel linguaggio comune, con valenza di scusa e di pretesto"[123].

Affinché l'alibi non venga considerato con la valenza di cui sopra, nel corso delle indagini sarà indispensabile che gli elementi raccolti siano coerenti e ragionevoli, tali da far assurgere l'alibi a valore di prova contro-deduttiva.

La fase di ricerca delle prove coinvolge direttamente le parti, gli organi inquirenti e - da non trascurare in relazione alle prove di natura informatica - il consulente tecnico, il cui ausilio risulta prezioso specialmente per i difensori (data la scarsa competenza in materia di quest'ultimi).

Il consulente di concerto con i soggetti predetti, dovrà:

- innanzitutto identificare tutte le possibili ipotesi ricavabili dai fatti acquisiti al procedimento ;
- verificare fattori come: i punti di forza o di debolezza, il grado di probabilità e la logica sottesi alle ipotesi individuate, in modo tale da rendere più agevole la verifica dei risultati, ma soprattutto l'attendibilità degli strumenti utilizzati;
- eseguire eventuali indagini suppletive con la finalità di integrare quegli ulteriori elementi probatori che possano essere di supporto alla tesi sostenuta e quindi in contrasto con le congetture della controparte;

123 E. COLOMBO, *La sentenza del caso di Garlasco e la computer forensics: analisi di un complesso rapporto tra diritto ed informatica,* in *Ciberspazio e diritto, 2010,* p. 452.

- infine, accertarsi che tutti gli elementi raccolti siano messi insieme secondo un unico criterio logico-giuridico, il più possibile coerente e motivato, tale da garantire che la loro acquisizione al processo possa avvenire in maniera non contraddittoria.[124]

Nel vecchio codice di rito a regime sostanzialmente inquisitorio, la raccolta delle prove nella fase istruttoria era effettuata solo dagli inquirenti.

La difesa dunque poteva soltanto controllare in dibattimento la regolarità degli atti compiuti e fare un'analisi critica delle prove raccolte, invece il Giudice aveva la facoltà di conoscere preventivamente gli atti istruttori e successivamente decideva su di essi.

Negli corso degli anni sono state diverse le leggi che pian piano hanno riconosciuto un maggior potere investigativo alla difesa.

Fu soprattutto a seguito della modifica dell'art. 111 Cost. (che ha introdotto il principio di parità e uguaglianza tra le parti), che si giunse all'approvazione della l. 397/2000[125] intitolata "Disposizioni in materia di indagini difensive".

La suddetta legge ha adottato una disciplina organica in materia, la cui importanza è stata sottolineata anche dalla Cassazione nel 2002[126], in cui la seconda Sezione della Suprema Corte ha affermato che la l. 397/2000 è "riconducibile al principio costituzionale di parità fra le parti

---

124 V. CALABRO', G. COSTABILE, S. FRATEPIETRO, M. IANULARDO, G. NICOSIA, "*Alibi informatico. Aspetti tecnici e giuridici "* in *IISFA Memberbook 2010,* pag.299

125 L. 7 dicembre 2000, n. 397, *Disposizioni in materia di indagini difensive,* reperibile sul sito *www.altalex.it.*

126 Cass., sez. II, 30 gennaio 2002 - 9 aprile 2002, n.13552, in *Cassazione Penale* 2003, p.1248.

processuali fatto proprio dall'art. 111 Cost. nel prevedere un'amplissima possibilità per i difensori delle parti private di assumere prove, delinea per le stesse una equiparazione – quanto ad utilizzabilità e forza probatoria, a quelle raccolte dalla pubblica accusa, sia nella fase delle indagini preliminari e dell'udienza preliminare che in quella dibattimentale.
[…] il Tribunale non può limitarsi ad acquisirli ma al fine di garantire l'effettività della difesa, ha l'obbligo di valutarle".

II.6.2 **Il ruolo dell'alibi informatico**

Questa breve disamina sull'attività di ricerca della prova esperibile dal difensore, ha la funzione di ben chiarire quanto proprio in presenza di un alibi si ribaltino le condotte dell'organo inquirente e della difesa: il primo dovrà infatti dimostrare l'infondatezza della prova portata a discredito della tesi dell'imputato, il secondo invece dovrà tentare in ogni modo di rafforzarne l'attendibilità.
Per capire in che modo si possa dimostrare la solidità o eventualmente l'inconsistenza di un alibi, nella fattispecie informatico, bisogna che durante le indagini la difesa - o meglio il più delle volte il consulente tecnico da questa incaricato - segua una sorta di schema analitico contenente diverse domande (ossia il *quis, quid*, *quando*, *ubi, cur, e il quomodo*) alle quali dovrà fornire adeguate risposte, per rendere la valutazione dell'alibi pienamente credibile e affidabile.
Prima di tutto l'alibi informatico deve essere "direttamente" riferibile all'imputato che lo fornisce a sua difesa, in caso contrario il rischio è che rimanga solo un indizio e non

assuma valore di prova.

Produrre documentazione informatica che riveli informazioni strettamente legate alla persona (transazioni autorizzate con dati biometrici, *pin o password,* documenti firmati digitalmente, immagini che ritraggono l'imputato), assume ad esempio un peso specifico maggiore rispetto ad un documento anonimo o ad un *log* che non rilevi alcun dato personale.

In secondo luogo, l'investigatore nel corso delle indagini ha il difficile compito di riuscire ad individuare, sulla base delle sue competenze, quali tracce informatiche possano costituire elementi di prova digitale.

La singola *digital evidence* infatti, non sempre è sufficiente a rappresentare una prova o un alibi, in tali circostanze sarà necessario ricercare fattori aggiuntivi anche esterni alla scena del crimine che abbiano la funzione di avvalorare o meno la stessa.

Per esempio una *email* acquista rilievo se può essere comprovata dai *log* dei *server* su cui è transitata, oppure dal traffico di rete generato.

Ancora, per valutare l'ammissibilità della prova, componente imprescindibile è il calcolo del "tempo ".

Riuscire a dimostrare che l'ora della formazione della prova è certa consente di mettere a confronto, in un intervallo temporale, la simultaneità dei tempi in cui si è consumato il reato oggetto del procedimento (Data di creazione, modifica e ultimo accesso, *log file, temporary file)*.

Anche il "luogo "è un elemento di rilievo, essere capaci infatti di palesare l'ambito in cui si sia formata una prova

informatica, potrebbe diventare significativo, qualora ad esso si potesse associare la presenza dell'imputato .

Spesso sono proprio le tracce relative ai luoghi che risultano facilmente modificabili, ad esempio per simulare la propria posizione in un determinato posto e in un determinato giorno, è sufficiente lasciare tracce informatiche (come quelle del cellulare, della carta di credito, del navigatore satellitare) le quali non richiedano la presenza contemporanea del soggetto.

Per quanto concerne il "perché", esso rappresenta il movente del reato, ma l'alibi può solo dimostrare che il movente non sia vero.

Infine, in merito alle "modalità", la prova informatica è oggettivamente un prodotto di strumenti tecnologici (*software,* palmari, rete dati, ecc..), per cui identificare ed analizzare le caratteristiche tecniche dello strumento utilizzato può rafforzare o indebolire la credibilità della prova stessa.

È chiaro che per il consulente tecnico attenersi in maniera scrupolosa a tale schema è impresa ardua, ma affrontare l'analisi della prova tentando di rispondere quantomeno alla maggior parte delle domande sopra citate, aiuterà a rappresentare una evidenza digitale in maniera completa e consentirà all'organo giudicante di potersi orientare con minor difficoltà circa l'ammissibilità o meno della prova[127].

---

127 V. CALABRO', G. COSTABILE, S. FRATEPIETRO, M. IANULARDO, G. NICOSIA, *Alibi informatico. Aspetti tecnici e giuridici* in *IISFA Memberbook 2010,* p. 312.

II.6.3 **Il "falso alibi"**

Finora però è stato menzionato l'alibi esclusivamente nella sua accezione positiva, ma di esso esiste anche un' accezione negativa degna di nota, ossia quella di "falso alibi".

Sulla rilevanza della falsità dell'alibi la giurisprudenza[128] si è espressa con opinioni non sempre omogenee e concordanti, ma malgrado ciò, deve constatarsi che "sia nel caso in cui esso sia stato artatamente preordinato o che si sia dimostrato puramente mendace, può essere posto in correlazione con altre circostanze di prova a carico e valutato come indizio nel contesto delle complessive risultanze probatorie, se appaia finalizzato alla sottrazione del reo alla giustizia".

Da ciò deriva, secondo la giurisprudenza, che l'alibi falso o mendacemente ricostruito non possa costituire prova a carico dell'imputato, ma possa essere valutato contro quest'ultimo solo se inserito in un più ampio quadro probatorio sfavorevole allo stesso come ulteriore fattore di valutazione del comportamento del medesimo, ossia dell'elemento soggettivo e soltanto ove vi sia appunto la certezza di falsità e mendacità.

Secondo i tradizionali cardini costituzionali quali "il principio del giusto processo"e "il diritto di difesa" questo orientamento non può ritenersi pienamente condivisibile, in quanto va a toccare il delicato tema del c.d. diritto dell'imputato a difendersi mentendo, ma soprattutto perché pone una commistione logica fra elementi fattuali ed elementi soggettivi che invece devono rimanere distinti.[129]

---

128 Cass.pen.,sez. II, 11 marzo 2004, n. 11840, in *CED 228386.*

129 F.CAJANI e S.ATERNO, *Aspetti giuridici comuni delle indagini informatiche,* dal testo *Computer forensics e Indagini digitali. Manuale*

L'allegazione di un alibi successivamente risultato falso sotto il profilo meramente fattuale, è assolutamente irrilevante (a meno che non si provi che la falsa predisposizione sia risalente al momento precedente o coevo alla commissione del reato) in quanto inidoneo ad influire sulla ricostruzione degli eventi.

D'altro canto decidere di formulare artificiosamente un falso alibi può solo testimoniare una condotta disonesta del soggetto, ma non può rappresentare la prova della sua reale colpevolezza poiché il comportamento processuale tenuto in seguito, non può dimostrare alcunché sugli elementi probatori attinenti alla commissione del fatto.

Dalle considerazioni sin qui effettuate, si può dedurre che tutto ha inizio dalle diverse strategie che la difesa decide di adottare a favore del proprio assistito.

Individuate le tesi ricostruttive, essa dovrà non solo trovare gli elementi di prova a loro sostegno, ma dovrà tenere altresì conto del fatto che potrebbe presentarsi l'impossibilità di procurarsi una determinata prova e per tale ragione dover apportare all'iniziale scelta difensiva "mutamenti di rotta ed adeguamenti".

Quindi, in realtà, l'elaborazione dell'alibi non sempre risulterà frutto di una scelta ricostruttiva originaria e definitiva, ma dovrà essere costantemente verificata ed adeguata soprattutto in fase di indagini preliminari, rispetto alle singole esigenze indiziarie e probatorie.

Peraltro, va precisato che per detta attività debbano essere utilizzate più tecniche e conoscenze in maniera coordinata e

---

tecnico-giuridico e casi pratici. Experta 2011.

coerente, visto che codesta vasta e articolata operazione dovrà riflettersi non solo sul grado di attendibilità dei dati ottenuti, ma anche sull'idoneità delle "metodologie" utilizzate, in quanto l'uso di più metodiche contemporaneamente può portare ad un ampliamento dei margini d'errore o di incertezza tali da indebolire l'alibi anziché rafforzarlo.

Proprio quest'ultimo sarà tema l'oggetto della prosieguo della trattazione, poiché è necessario comprendere in che modo procedure scorrette attuate durante l'applicazione delle metodologie informatiche incidano sulle garanzie processuali e anche sul libero convincimento del Giudice.

II.7 "Malpractices" nella digital forensic: giurisprudenza a confronto.I

La valutazione di una prova scientifica, qualunque sia la sua finalità (ricostruzione di un fatto, spiegazione delle cause di un evento, accertamento dello stato di un luogo ecc...) è un tema che riguarda non solo il momento della decisione, ma anche le fasi precedenti.

La prima fase è quella dell'accertamento della validità della prova o tecnica scientifica da utilizzare nel processo.

Tale accertamento spesso non viene effettuato poiché la validità della prova è data per implicita, ma "diventa fondamentale quando le tecniche eseguite siano particolarmente avanzate o oggettivamente controverse".[130]

La seconda fase è quella caratterizzata dalla verifica della

130 C. BRUSCO, *La valutazione della prova scientifica,* in *Diritto penale e processo* 2008, p.23.

teorica idoneità della prova scientifica a fondare un accertamento processualmente valido, capace di fornire indicazioni quanto più utili possibili.

La terza ed ultima fase è contraddistinta dalla valutazione del risultato della prova che costituisce probabilmente il tema più delicato dell'esperienza giudiziaria, soprattutto per l'avanzare del sapere scientifico e per la presenza nel nostro ordinamento di strumenti processuali particolarmente adatti alla ricerca della *digital evidence*[131]: in particolare, ci si riferisce all'art. 189 c.p.p. il quale stabilisce che quando è richiesta una prova non disciplinata dalla legge, il giudice possa assumerla se essa risulta idonea ad assicurare l'accertamento dei fatti.

Con attenzione alla prima fase, a garanzia del diritto di difesa diventa di primaria importanza accertarsi delle modalità con cui la prova viene acquisita, specie laddove il suo contenuto sia talmente tecnico da non lasciare spazio ad argomentazioni difensive di merito.

Fin dall'inizio dell'attività di acquisizione della prova, gli inquirenti incorrono in quei rischi derivanti dai due caratteri propri dei dati digitali quali come già più volte accennato:

"l ' immaterialità e la fragilità".

L'immaterialità è data dalla natura aleatoria della traccia informatica, mentre la fragilità rende quest'ultima facilmente alterabile, danneggiabile e distruttibile, indipendentemente da manipolazioni su di essa di origine dolosa o colposa.[132]

---

131 O. DOMINIONI, *In tema di nuova prova scientifica,* in *Diritto penale e processo* 2001, p.1061

132 M. A. SENOR, *Legge 18 marzo 2008, n. 48 di ratifica ed esecuzione della Convenzione di Budapest sulla criminalità informatica: modifiche al codice di procedura penale ed al d.lgvo 196/03,* in *www.penale.it*

Da tale scenario emerge la necessità di preservare scrupolosamente l'integrità delle impronte digitali, che spesso è messa a rischio proprio dagli stessi investigatori o esaminatori non sempre adeguatamente preparati, con la conseguenza di fornire alla difesa dell'indagato ampie possibilità di infondere il dubbio all'organo giudicante sulla genuinità dell'*iter* di formazione della prova.

Questa realtà virtuale di difficile gestione presenta un altro limite insito nell'attività investigativa, relativo alla costante evoluzione tecnologica a cui gli strumenti impiegati sono esposti, la quale rende ben presto obsolete e inefficaci le tecniche utilizzate.

Per queste ragioni agli investigatori è richiesta l'adozione di determinate cautele, dettate da procedure standardizzate elaborate dalla comunità scientifica internazionale e un aggiornamento tecnico–scientifico continuo, proprio per stare al passo con l'incedere tecnologico.

II.7.1 **Gli standard di tutela della prova digitale e il caso *Vierika***

A tal proposito la legge 48/2008, come già osservato nel corso della presente trattazione, ha introdotto precisi parametri di garanzia per tutelare l'acquisizione e la preservazione delle *digital evidence.*

In particolare i nuovi *standard* possono essere condensati in tre fondamentali previsioni: *a*) dovere di preservare il dato originale nella sua genuinità; *b*) dovere di impedire l'alterazione della fonte di prova originale; *c*) dovere di acquisire il dato mediante procedure che assicurino la

conformità della copia all'originale.

Il problema che la disciplina pone, tuttavia, è la mancata determinazione di quali effetti conseguano al mancato rispetto di tali prescrizioni[133], ma anche quale valore attribuire ad eventuali scorretti reperimenti delle fonti di prova.

In virtù dei pericoli sottesi alla fase di acquisizione delle prove digitali, sarebbe opportuno che la giurisprudenza prendesse posizioni meno contestabili in ordine alla valutazione delle risultanze informatiche[134].

Sin dal *leading case* "*Vierika* "[135], invece, si è potuta constatare una certa reticenza da parte dei nostri giudici verso una corretta gestione del dato informatico, e proprio in tale sentenza per la prima volta un giudice italiano si è trovato a dover rispondere al quesito relativo alla sorte processuale di una risultanza probatoria informatica, ottenuta senza seguire le *best practices.*

Nel caso di specie l'imputato era stato accusato di aver messo in circolazione un *worm*[136] denominato appunto *Vierika,* in grado di diffondersi automaticamente attraverso l'invio inconsapevole di *e-mail* da parte dei *personal computer,* di quanti avessero incautamente aperto l'allegato "infetto".

Ebbene nel caso giudiziario in esame, la difesa aveva a più riprese contestato la correttezza delle metodologie utilizzate

133 D. LA MUSCATELLA, *La ricerca della prova digitale e la violazione delle best practices: un'attività investigativa complessa tra recenti riforme e principi consolidati,* in *Ciberspazio e diritto* 2011, p. 222.

134 L. MARAFIOTI, *Digital evidence e processo penale,* in *Cassazione penale* 2011, p.4521

135 Trib. Bologna, 22 dicembre 2005, n. 1823, in *www.penale.it.*

136 Un *worm* (letteralmente verme) è una particolare categoria di *malware* in grado di autoreplicarsi. È simile ad un *virus* ma a differenza di questo non necessita di altri *file* per diffondersi.

dalla polizia giudiziaria per l'estrazione dei *files* dall'elaboratore dell'imputato e per la raccolta dei flussi telematici, giudicate difformi dalla migliore pratica scientifica e inidonee a garantire all'accusato una forma di effettivo contraddittorio, anche a causa della ipotizzata irripetibilità delle operazioni effettuate.

Ciononostante, il giudice di merito optò per respingere tali contestazioni a seguito di due princìpi di diritto alquanto discutibili.

Il primo si riassume nell'affermazione secondo cui non è compito dell'organo giudicante verificare la corrispondenza dei criteri impiegati nelle indagini tecniche rispetto ai protocolli di *best practices*.

Il secondo consiste nell'enunciazione della regola in base alla quale anche qualora dovessero rilevarsi delle differenze rispetto agli *standard* internazionali, "graverebbe comunque sull'imputato *l'onus probandi* di dimostrare, quale concreta alterazione del dato informatico si fosse verificata"[137].

A corollario di queste premesse la sentenza in oggetto ha poi aggiunto un'ulteriore *regula iuris*: il reperimento delle prove digitali, seppur attuato in difetto ai modelli teorici più corretti, non può in ogni caso costituire causa di inutilizzabilità, ma solo un motivo per indurre il giudice a far ricorso ad elementi di riscontro e di convalida nel momento della decisione.

Alla luce dei princìpi cui si ispira il nostro sistema di giustizia penale, le conclusioni cui è giunto il tribunale

---

137 L. LUPARIA, *Il caso "Vierika": un'interessante pronuncia in materia di virus informatici e prova penale digitale. I profili processuali;* in *Diritto dell'Internet,* 2005, p. 153.

monocratico appaiono fortemente criticabili.

In primo luogo, infatti, un giudice che rimanga inerte dinnanzi all'ingresso dibattimentale della prova tecnico-scientifica, si pone in netto contrasto con quella "cultura dei criteri",[138] ritenuta coessenziale al vaglio giurisdizionale sulla idoneità probatoria della *digital evidence* e avvalorata dalla raccomandazione al giudice "di porsi il problema della verifica della effettiva validità scientifica dei criteri e dei metodi d'indagine e della loro conseguente affidabilità processuale"[139].

Del resto, anche nell'ordinamento giuridico di *common law*, dove queste tematiche vengono affrontate con particolare attenzione da diversi anni, risulta pacifico che al giudice spetti l'incisivo ruolo di *gatekeeper*[140] nei riguardi degli accertamenti ad alto contenuto tecnologico, la cui affidabilità deve appunto essere apprezzata sulla scorta dei protocolli elaborati dalla comunità scientifica[141].

Parimenti discutibile appare poi anche la seconda prospettiva

---

138 O. DOMINIONI, "la cultura dei criteri" consiste in schemi concettuali intesi a scrutinare la validità delle leggi scientifiche e delle tecnologie usate dall'esperto e la loro corretta applicazione. Spetta allo stesso giudice enucleare questi criteri, che può attingere dall'elaborazione giurisprudenziale, dalla letteratura giuridica, dalla *forensics science*, dallo stesso ambito scientifico, posto che gli studiosi nel definire un nuovo principio scientifico o un nuovo metodo tecnologico, intanto ne accreditino la validità mettendo a punto anche gli indici della loro verifica, in *La prova penale scientifica: gli strumenti scientifico-tecnici nuovi o controversi e di elevata specializzazione,* Giuffrè 2005.

139 L. LUPARIA, *Il caso "Vierika": un'interessante pronuncia in materia di virus informatici e prova penale digitale. I profili processuali;* in *Diritto dell'Internet,* 2005*,* p. 153

140 G .CANZIO, *Prova scientifica, ragionamento probatorio e libero convincimento del giudice nel processo penale,* in *Diritto penale e processo* 2003, p.1194.

141 O. DOMINIONI, *La prova penale scientifica: gli strumenti scientifico-tecnici nuovi o controversi e di elevata specializzazione,* Giuffrè 2005.

teorica fatta propria dalla decisione in questione.

Si colloca in effetti fuori dal sistema del nostro ordinamento processuale, l'apposizione a carico della difesa di un onere di prova, circa le esatte modificazioni del dato digitale causate dallo scostamento dalle *best practices.*

La tutela della genuinità della *digital evidence* costituisce infatti un valore assoluto al quale devono conformarsi gli organi inquirenti[142], pena l'inutilizzabilità del materiale raccolto per inidoneità delle evidenze a garantire un accertamento affidabile dei fatti di reato.

L'imputato deve limitarsi a dimostrare che le tecniche eseguite per l'acquisizione, per la conservazione e la successiva elaborazione della *chain of custody,* non rispecchino i criteri solitamente riconosciuti come attendibili.

Ove ciò si verifichi, incomberà sull'accusa il compito di provare che quel metodo, seppur difforme dalla miglior prassi tecnica, non abbia modificato i dati e salvaguardato la c.d. "integrità digitale"[143]; e qualora si presentino delle perplessità su quest'ultima evenienza, si dovrà accogliere "la regola di giudizio dell' in *dubio pro reo* e non certo quella secondo cui *in dubio pro republica "*[144].

Infine è da evidenziare il terzo aspetto di interesse della motivazione, ossia il riferimento del giudice all' art. 192, 1° comma c.p.p.

---

142 Art. 13 della *Raccomandazione R (95)13* dell'11 settembre 1995 redatta dal Comitato dei Ministri del Consiglio d'Europa, reperibile sul sito *www.gnosis.aisi.gov.it.*

143 G. COSTABILE - D. RASETTI, *Scena criminis, tracce informatiche e formazione della prova,* in *Cyberspazio e diritto,* 2003*,* p. 278

144 L. LUPARIA, *Il caso "Vierika": un'interessante pronuncia in materia di virus informatici e prova penale digitale. I profili processuali;* in *Diritto dell'Internet,* 2005*,* p. 153.

Secondo il ragionamento seguito nella pronuncia in analisi, tale norma consentirebbe appunto al giudice di ammettere la valutazione anche di quelle evidenze digitali raccolte in violazione dei corretti *standard* scientifici di acquisizione.
Il concretarsi di condotte capaci di influire sulla genuinità della prova, comporterebbe per l'organo giurisdizionale quindi il solo obbligo di corroborare tale materiale "spurio", tramite ulteriori elementi in grado di avvalorarne l'attendibilità.
Ebbene tale ricostruzione va senz'altro contrastata.
L'unica risposta plausible dell'ordinamento processuale ad una prova formata senza il necessario rispetto dell'integrità della stessa, è una declaratoria di inutilizzabilità probatoria ai sensi dell'art. 191 c.p.p., e dei princìpi in materia di salvaguardia dell'integrità della prova digitale introdotti dalla l.48/2008.
Non deve mai essere possibile in altre parole compensare la scarsa "qualità" delle prove con una maggiore "quantità" delle stesse, né esse possono, sulla base di un erroneo utilizzo della categoria degli indizi, concorrere alla formazione del libero convincimento del giudice.

II.7.2 **Il caso di Garlasco**

Anche le pronunce più attente al profilo della genuinità del dato digitale non sembrano sinora essersi allontanate dalla retroguardia di un disinvolto utilizzo del libero convincimento del giudice, come unica risposta possibile dinanzi eventuali abusi in sede di raccolta.

A conferma di questa affermazione può prendersi in esame un altro caso, noto come "Il delitto di Garlasco"[145], nel quale si denota un comportamento da parte degli organi inquirenti e del giudice non dissimile da quello attuato nel caso *Vierika.*

Nel caso di specie, in data 13 agosto 2007 Chiara Poggi, 26 anni, venne brutalmente uccisa con un oggetto contundente.

L'unico soggetto su cui si concentrarono le indagini fu il suo fidanzato Alberto Stasi, il quale tuttavia fornì a sua difesa un alibi poco convincente.

La persona sottoposta alle indagini sostenne infatti di trovarsi nel proprio appartamento a lavorare al *computer* alla sua tesi, proprio nelle ore in cui si era presumibilmente verificato il decesso della giovane.[146]

Ai fini del presente lavoro risulta di particolare interesse l'aspetto inerente alla consegna in data 14 agosto 2007 da parte di Stasi del proprio *computer* portatile alla polizia giudiziaria: da quel momento fino al 29 agosto 2007 (data in cui il reperto informatico è stato consegnato ai consulenti tecnici del Pubblico Ministero per l'effettuazione delle copie forensi del contenuto del supporto), infatti, la P.G. ha proceduto a degli accessi scorretti e ripetuti, in contrasto con i protocolli operativi riconosciuti dalla comunità scientifica, rilevabili già nella ricostruzione delle operazioni svolte dai militari nel verbale del 29 agosto 2007 .[147]

---

145 Tribunale di Vigevano 17 dicembre 2009, reperibile sul sito *http://static.repubblica.it/laprovinciapavese*/pdf/*SENTENZA_STASI*.pdf.

146 L. MARAFIOTI; *Digital evidence e processo penale,* in *Cassazione penale* 2011, p.4522.

147 E.COLOMBO, *La sentenza del caso di Garlasco e la computer forensics: analisi di un complesso rapporto tra diritto ed informatica,* in *Ciberspazio e diritto* 2010, p. 449.

All'esito dei successivi accertamenti tecnici furono riscontrati sette accessi al *personal computer* di Stasi, l'installazione ed utilizzo di alcune periferiche *USB,* nonché accesi multipli al *file* della tesi di laurea in vari percorsi di memorizzazione.

Queste scorrettezze sono state chiaramente evidenziate in prima battuta nella relazione del collegio peritale informatico, indi sono state riscontrate anche dai consulenti tecnici del P.M. (i RIS di Parma) nella loro successiva analisi.

Le procedure adottate erroneamente dalla polizia giudiziaria nell'attività svolta sul *P.C.* dell'indagato, hanno portato la difesa di Stasi ad eccepire numerosi dubbi a seguito dei quali il giudice decise di disporre una perizia, al fine di effettuare copie conformi all'originale per accertare l'inalterabilità e l'immodificabilità dei dati dei supporti informatici. Il giudice inoltre richiese di evidenziare le alterazioni di contenuto dei dati stessi e di quantificare le perdite di evidenze digitali.

Come risultato dall'escussione testimoniale dei periti nominati nell'immediatezza dell'intervento della P.G. e mediante l'accertamento sul PC di Stasi, venne stimata una perdita definitiva superiore alla metà dei dati informatici in esso contenuti.

Nonostante questa circostanza il giudicante ritenne comunque attendibili le risultanze delle acquisizioni informatiche ottenute, in quanto a suo giudizio reperite dai militari secondo “buonafede”.

Probabilmente non si è tenuto però debitamente conto delle dannose conseguenze che si possono essere prodotte anche sui dati rimasti (forse!) integri e genuini, all'esito di un

intervento acquisitivo scientificamente contestabile, primo fra tutti quella di dare origine ad un procedimento iniquo e inefficace.

Da quanto rilevato, emerge come le Forze dell'Ordine del nostro ordinamento (a differenza di quanto accade negli ordinamenti di USA e UK) abbiano redatto delle linee guida di intervento per le indagini informatiche dettate però al solo fine dell'uso interno, che non hanno quindi carattere di ufficialità e cogenza.

Dal confronto tra i due casi (Vierika-Garlasco) è chiaro come si vada a creare un rischioso intreccio tra "libertà di acquisizione" e "libertà di valutazione " da parte dei giudici, che hanno scelto di utilizzare dei risultati di *digital evidence,* nonostante le scorrettezze realizzate nell'attività acquisitiva, con il risultato di aver spostato la questione della genuinità della prova digitale sul terreno della valutazione e non su quello dell'inutilizzabilità.

Queste azzardate e rischiose decisioni fatte proprie da entrambi i giudici, hanno posto in essere un quesito di non facile soluzione circa il ruolo che dovrebbe assumere il giudice in casi specifici in cui rientrino materie scientifiche e tecnologiche.

Le risposte non sono univoche.

C'è chi[148] sostiene che il livello delle conoscenze tecnico-scientifiche del giudice dovrebbe assolutamente elevarsi.

Egli, in quanto gravato dal ruolo di *peritus peritorum,* ha il difficile compito di interrogare reiteratamente la comunità

148 G. CANZIO, *Prova scientifica, ragionamento probatorio e libero convincimento del giudice nel processo penale,* in *Diritto penale e processo* 2003, p.1199.

scientifica e di rielaborare le risposte informative: all'esito, dovrebbe interpretare i dati scientifici e testarne l'affidabilità, non in condizione di recettore passivo bensì secondo le esigenze di giustizia e nell'interesse pratico di risolvere la specifica controversia.

D'altro canto c'è anche chi[149] ritiene che il giudice non debba sostituirsi all'esperto o compiere *ex novo* il percorso dal medesimo compiuto, ma debba riuscire a valutare sia la validità dei metodi scientifici utilizzati, sia le condizioni secondo le quali attribuire ad un'informazione tale validità.

II.7.3 **Prospettive attuali**

La più recente ricerca ha individuato nel metodo critico esercitato nel contraddittorio delle parti, quello più idoneo a risolvere problemi di ammissione, assunzione e valutazione della prova scientifica.

Il metodo da ultimo menzionato, utilizzato in tutte le fasi citate, costituisce espressione forte di un contraddittorio, che non risponde soltanto all'esigenza di garantire la parità fra le parti, ma rappresenta il miglior "metodo epistemologico per la ricerca della verità processuale"[150], tanto più quando vengano utilizzati nel processo strumenti probatori controversi.

Forse dunque, accantonata la visione tradizionale ed illusoria del giudice *peritus peritorum,* sarebbe opportuno intendere l'organo giudicante come un soggetto pronto ad esaminare

149 C. BRUSCO, *La valutazione della prova scientifica,* in *Diritto penale e processo* 2008, p. 28.

150 P. TONINI, *Progresso tecnologico, prova scientifica e contraddittorio,* in *Diritto penale e processo* 2003, p.1459.

visioni scientifiche diverse e a scegliere quella più convincente, non in base ad un'opzione pregiudiziale e immotivata ma, dopo aver dato il più ampio spazio al contraddittorio, aderendo così alla posizione fondata su una dimostrata attendibilità scientifica e su argomentazioni che non abbiano trovato obiezioni insuperabili[151].

A seguito di tale deduzione (posto che la libertà del giudice di elaborare il proprio convincimento senza vincoli passa attraverso l'obbligo di manifestare, in forma scritta, il percorso con cui quel convincimento è stato raggiunto), con riferimento al dispositivo della sentenza di Garlasco in cui si legge la formula di assoluzione per l'imputato "per non aver commesso il fatto", forse ci si sarebbe attesi una formula dubitativa e*x* art. 530, comma 2° c.p.p., considerati gli omessi tecnicismi acquisitivi dei dati informatici che hanno dato adito alle obiezioni precedentemente esaminate.[152]

In conclusione, appare irrinunciabile la necessità oltre che di protocolli seguiti con maggiore attenzione e professionalità, anche di "un'etica" condivisa da parte di tutti i soggetti coinvolti all'interno di un processo penale, che "funga da barriera a manipolazioni, deformazioni, omissioni e contaminazioni, i cui effetti dirompenti sono da tutti intuibili se si considera l'oggetto del processo e le sue implicazioni, ossia la possibile condanna di un innocente o, al contrario, l'assoluzione di un colpevole".[153]

---

151 C. BRUSCO, *La valutazione della prova scientifica,* in *Diritto penale e processo* 2008, p. 28.

152 E. COLOMBO, *La sentenza del caso di Garlasco e la computer forensics: analisi di un complesso rapporto tra diritto ed informatica,* in *Ciberspazio e diritto* 2010, p. 460.

153 S. LORUSSO; *Investigazioni scientifiche, verità processuale ed etica degli esperti,* in *Diritto penale e processo* 2010, p.1349.

II.7.4 **La Cooperazione internazionale nella lotta contro la criminalità organizzata:**

I recenti processi di globalizzazione i quali hanno comportato il graduale depotenziamento delle frontiere e il sempre più libero e incontrollato trasferirsi delle persone e dei beni, hanno avuto una notevole ricaduta sullo sviluppo e sulle interconnessioni fra le economie e i soggetti criminali dei vari paesi, accentuando il carattere sistemico delle relazioni tra le società e gli Stati[154].

Conseguenza di questo fenomeno è stato il superamento, nelle forme delinquenziali, della dimensione "individuale" e la diffusione di quella organizzata-complessa che, peraltro, si va sempre più strutturando, quanto a dinamiche operative, su schemi transnazionali.

Con il termine "transnazionalità" si intende alludere alla cooperazione che gruppi criminali di diversa nazionalità instaurano tra di loro, per gestire più efficacemente determinati mercati criminali.

I crimini transnazionali assumono differenti manifestazioni: in primo luogo alcuni reati sono da considerarsi come transnazionali in *re ipsa*, come accade nel caso dei cosiddetti *cross-border crimes* (traffico illecito di armi, di droga, tratta di esseri umani), la cui commissione postula di necessità l'attraversamento di una o più frontiere tra Stati[155].

Per altre fattispecie il requisito della transnazionalità è da

---

154 BARTONE, *Mandato di arresto europeo e tipicità nazionale del reato*, Milano, 2003, p.4 ss., in *Mandato di arresto europeo e procedure di consegna* (a cura di Kalb), Milano, 2005.

155 A. DI MARTINO, *La frontiera e il diritto penale. Natura e contesto delle norme di diritto penale transnazionale,* Torino, 2006, p. 67 ss.

ricollegare al luogo in cui si verifica l'offesa del bene giuridico tutelato, basti pensare ai reati ambientali attuati mediante trasferimento da uno Stato all'altro di rifiuti tossici.
In ultimo ed oggetto si colloca la tipologia di reati transnazionali relativa ai *cybercrimes.*
In merito ai reati poc'anzi citati, la collaborazione criminale è resa estremamente facilitata proprio dall'utilizzo di *Internet* il quale, per sua stessa natura, si presta a costituire un efficiente veicolo per la consumazione di reati che travalichino - in maniera virtuale - le frontiere tra gli Stati.
Molti degli Stati che hanno ratificato la Convenzione di Budapest, in quanto altresì membri dell'Unione Europea, sono tenuti a rispettare una serie di accordi in tema di cooperazione giudiziaria penale.
Già con il Trattato di *Maastricht* del 1992, per arginare l'espansione del fenomeno transazionale di numerosi crimini, si era provveduto a predisporre strumenti normativi nell'ambito del Terzo Pilastro dell'Unione, contro le principali condotte criminose, attraverso l'elaborazione di definizioni comuni delle più gravi figure delittuose[156].
In quest'ottica si colloca l'Azione comune 733/98/GAI[157] contro la criminalità organizzata, adottata dal Consiglio dell'Unione Europea il 21 dicembre 1998, tesa a rafforzare – nel rispetto dei diritti fondamentali riconosciuti e tutelati dalla Convenzione Europea per la salvaguardia dei diritti dell'uomo – la cooperazione tra gli Stati membri nella lotta a

156 L.SALAZAR, *La lotta alla criminalità nell'Unione: passi in avanti verso uno spazio giudiziario comune prima e dopo la Costituzione per l'Europa ed il Programma dell'Aja,* in *Cassazione penale*, 2004, p. 3513 ss.
157 Reperibile sul sito www.eur-lex.europa.ue., cod.31998F0733.

gravi forme delinquenziali a carattere associativo[158].

Nell'anno successivo (1999) in sede del vertice di Tampere venne creata *Eurojust,* l'unità di cooperazione giudiziaria permanente con lo scopo di coordinare le indagini a livello comunitario; degno di menzione è anche *Europol* quale ufficio europeo di polizia, il quale ha come obiettivo principale quello di facilitare lo scambio di dati tra ufficiali di collegamento dei singoli Stati Membri attraverso un'analisi di *intelligence*, rilevano ancora la previsione delle procedure di mandato d'arresto europeo e di mandato di ricerca della prova, il Trattato di *Prum* del 2005 per la protezione e lo scambio dei dati; l'istituzionalizzazione di un nuovo sistema di informazioni *Schengen* chiamato SIS II, il cui sistema è composto da una banca dati, gestita a Strasburgo, che consente di diramare in brevissimo tempo informazioni su persone e oggetti ricercati ed infine, una pluralità di altri accordi unilaterali e bilaterali con gli altri Stati, con il medesimo fine di rendere sempre più efficiente una cooperazione giudiziaria internazionale[159].

Nel quadro normativo europeo, si colloca anche il capitolo terzo della Convenzione di Budapest 2001, il quale definisce e regola la materia della cooperazione internazionale e della mutua assistenza tra gli Stati nella lotta ai crimini commessi con l'uso dei mezzi e sistemi informatici[160].

---

158 S.ATERNO, F.CAJANI, *Aspetti giuridici comuni delle indagini informatiche,* dal testo *Computer forensics e indagini digitali.* Experta, 2011, p.170 ss.

159 E.COLOMBO, *La cooperazione internazionale nella prevenzione e lotta alla criminalità informatica: dalla Convenzione di Budapest alle disposizioni nazionali,* in *Ciberspazio e diritto,* 2009, p. 301.

160 F.CAJANI, *Verso un nuovo concetto di cooperazione internazionale,* dal testo *Computer forensics e Indagini digitali. Manuale tecnico giuridico e casi pratici,* Experta, 2011, p.164

Le disposizioni contenute in questo capitolo, legittimano e specificano le regole di applicazione dei tradizionali strumenti di cooperazione, già in vigore tra gli Stati (si pensi, in tal senso, all'estradizione) e prevedono le linee guida da applicare nella cooperazione tra Paesi, ove non siano già vigenti delle politiche di indirizzo comuni. In quest'ultima ipotesi, trovano applicazione soltanto le norme della Convenzione di Budapest[161].

L'obiettivo principale perseguito dalla Convenzione in tale ambito è quello di "armonizzare" il più possibile le procedure e le disposizioni di mutua assistenza, ma seguito di un'analisi comparatistica condotta tra alcuni Stati ratificanti, sarà possibile constatare come questo obiettivo risulti di difficile attuazione con conseguente maggiore o minor adeguamento all'accordo pattizio.

In Italia, per es., la legge di ratifica all'art. 2, contiene un'esplicita previsione di " piena ed intera" esecuzione alla Convenzione di Budapest.

In tema di cooperazione internazionale, però, la suddetta previsione risulta quasi del tutto inapplicata[162]: restano infatti privi d'attuazione gli artt. 26, 28, 30, 31, 32, 33, 34.

Si può notare una corretta attuazione soltanto dell'art.35 della Convenzione, mediante l'istituzione del punto di contatto 24/7 da parte del Ministro dell'Interno, di concerto con il Ministro della Giustizia. È previsto, infatti, un *network 24/7* in ogni Stato, per accelerare il traffico di dati, al fine di una

161 E.COLOMBO, *La cooperazione internazionale nella prevenzione e lotta alla criminalità informatica: dalla Convenzione di Budapest alle disposizioni nazionali,* in *Ciberspazio e diritto,* 2009, p. 290ss.

162 Cfr. *Tabella dei profili dello Stato* a cura del Consiglio di Stato, reperibile sul sito *www.coe.int/cybercrime*.

più proficua cooperazione contro la lotta alla criminalità informatica.

Nello specifico, tale punto informativo deve risultare disponibile 24 ore su 24 e 7 giorni su 7 " per assicurare un'assistenza immediata per le indagini relative a reati connessi a sistemi informatici e dati informatici, o per la raccolta di prove in formato elettronico di un reato"[163].

Per l'Italia il compito è svolto da una struttura operativa presso il Servizio di polizia postale e delle comunicazioni della Polizia di Stato.

La previsione di una *task force* perennemente operativa fu il frutto di un fitto dibattito sviluppatosi intorno agli '80 "sulle modalità attraverso cui conseguire una omogeneizzazione delle fattispecie incriminatrici presenti all'interno dei singoli Stati ed introdurre forme di rapida collaborazione per le evidenze necessarie a sostenere le accuse nei giudizi per i reati informatici".

In seguito si sono sviluppate esperienze concrete come quella dell' *High tech subgroup,* creata all'interno del G8.

Proprio da quest'ultimo nasce il *network 24/7* inserito nella Convenzione.

Questo punto di contatto è chiamato a fornire un'assistenza che si traduce in primo luogo, nel garantire l'apporto di consigli tecnici per le attività connesse alla repressione dei crimini informatici.

In secondo luogo, l'assistenza serve per la conservazione dei

163L.CORDI', L.18/03/2008 n.48 – Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno (G.U 4.4.2008 n.80)", in Legislazione Penale 2008, p.321

dati secondo quanto disposto dagli artt. 29 e 30 della Convenzione.

Infine, cura anche la raccolta di prove, la trasmissione di informazioni e la localizzazione dei sospetti.

Quest'ultimo è un profilo particolarmente delicato sul quale occorre fare un cenno a se stante.

Nello spazio europeo, infatti, la trasmissione delle informazioni soprattutto in ambito penale, comporta la circolazione di dati strettamente personali quindi indubbiamente "sensibili".

A tal riguardo, l'Unione si è mossa secondo due diverse linee direttrici, la prima, definita "tutela della sicurezza interna", la seconda, "tutela della sicurezza dei dati personali"[164].

Sul primo versante l'obiettivo perseguito è stato la protezione della collettività di fronte al crimine, sul secondo versante, invece, si è avuto riguardo agli interessi cui i dati delle persone si riferiscono.

Proprio lo "sdoppiamento" della tutela prevista dall'Unione, però, denota come ancora una volta e nonostante i passi fatti in avanti, essa abbia rinunciato in una logica strettamente compromissoria ad elaborare una disciplina unica nel settore della cooperazione informativa nell'ambito della giustizia penale, lasciando ai singoli Stati il difficile compito di predisporre adeguati *standards* di tutela.

A sostegno di quanto detto, basti pensare al programma di rafforzamento degli scambi di informazione in materia di condanne penali, ravvisabile nel "pacchetto legislativo globale" proposto dalla Commissione europea nel periodo

164 G.DI PAOLO, *La circolazione dei dati personali nello spazio giudiziario europeo dopo Prum,* in *Cass. pen.,* 2010*, p.*1973

2005-2008, rapidamente tradottosi nell'adozione di ben tre diversi testi normativi: la decisione quadro 2008/675 GAI, relativa alla considerazione delle decisioni di condanna tra Stati Membri dell'UE in occasione di un nuovo procedimento penale; la decisione quadro 2009/315/GAI, concernente l'organizzazione e il contenuto degli scambi tra Stati Membri di informazioni estratte dal casellario giudiziario; infine la decisione quadro 2009/316/GAI, che istituisce il sistema europeo di informazione dei casellari giudiziari (ECRIS)[165].

Anche in questo caso,infatti, malgrado l'azione dell'Unione nel settore dello scambio di informazioni relative alle condanne penali sia stata molto determinata, nella decisione quadro in ultimo menzionata è emerso come la realizzazione di ECRIS, a prescindere dalla predisposizione di un adeguato sistema di protezione dei dati personali, non sia riuscita ad offrire un livello omogeneo di protezione rispetto ad informazioni di carattere "sensibile", consentendo alla logica "securitaria" di prevalere sul rafforzamento delle garanzie individuali.

Tornando alla disamina comparativa sull'adeguamento alla Convenzione di Budapest da parte degli Stati ratificanti, l'attenzione si deve focalizzare su Francia e Germania.

La prima, ha ratificato l'Accordo internazionale in data 10 gennaio 2006[166].

Le modifiche e le integrazioni alla legislazione già vigente,

---

165 G.DI PAOLO, *La circolazione dei dati personali e del casellario giudiziario,* in *Cass. pen,* 2001, p.4040 ss.

166 E.COLOMBO, *La cooperazione internazionale nella prevenzione e lotta alla criminalità informatica: dalla Convenzione di Budapest alle disposizioni nazionali,* in *Ciberspazio e diritto,* 2009, p. 295

sono state piuttosto esigue, poiché le norme interne sono risultate già conformi alla Convenzione.

In riferimento alla cooperazione internazionale, sono state introdotte poche e semplici disposizioni nel codice di procedura penale.

Unica previsione della Convenzione rimasta inattuata è l'art. 35, circa l'istituzione del punto di informazione 24/7 e questo non è elemento di poco conto, se si pensa che tale *network* è uno strumento fondamentale e coadiuvante della mutua assistenza e della più rapida ed efficiente circolazione dei dati nel ciberspazio.

Nell'ulteriore comparazione con la Germania, invece, emerge come si conformi ed applichino le disposizioni della Convenzione, con la sola vigenza dei codici e delle leggi interne.

Per la materia di cooperazione internazionale, il riferimento è alla legge di assistenza giudiziaria internazionale in materia penale (IRG)[167] la quale corrisponde perfettamente agli artt. dal 24 al 31, 33 e 34 della Convenzione e all'art. 94 del codice di rito tedesco.

È stato anche stabilito il punto di contatto 24/7, presso gli uffici del *Bundeskriminalamt.* La Germania è anche membro del G8 1995/1996 e dell'ICPO *Interpol.*

Fuori dal panorama europeo, meritano un accenno gli Stati Uniti d'America*,* primo Stato in cui si sono verificati episodi di criminalità informatica. Essi hanno proceduto alla ratifica della Convenzione, in data 29 settembre 2006.

167 Tale legge del 23 dicembre 1982, si compone di 11 articolati capitoli e di 98 paragrafi in materia di mutua assistenza giudiziaria in materia penale. Testo integrale, reperibile sul sito http://www.gesetze-im-internet.de/irg/BJNR020710982.html

Non si trova, però, all'interno dell'ordinamento giuridico Statunitense, alcuna corrispondenza con le disposizioni dell'accordo internazionale, in materia di cooperazione internazionale, soltanto la procedura per l'estradizione presenta una normativa dettagliata.

In considerazione della notoria posizione degli Stati Uniti d'America a livello mondiale, questo mancato adeguamento all'interno dell'ordinamento giuridico dei medesimi, può considerarsi un ostacolo per una collaborazione realmente efficiente e globale contro il dilagante fenomeno criminale transfrontaliero.

Sempre nel contesto europeo, degna di nota, appare la "Raccomandazione del Parlamento europeo del 26 marzo 2009", destinata al Consiglio, che ha ad oggetto il rafforzamento della sicurezza e della libertà fondamentali su *Internet*, al fine di garantire un pieno e sicuro accesso alla rete da parte di tutti e di combattere la cibercriminalità, con l'invito all'adozione di strategie globali, conformi alle direttive della Convenzione e, altresì, con l'incoraggiamento alla cooperazione tra esponenti del settore pubblico e privato anche a livello internazionale.

La Commissione europea molto attenta ai problemi suddetti, ha previsto l'istituzione di una *European Alert Platform* operativa dal 2009, con il fine di realizzare progetti in tale ambito mediante lo stanziamento di fondi comunitari.

Ancora nel "G8 Giustizia e Affari interni" tenutosi a Roma nel maggio 2009, nella dichiarazione conclusiva, i Ministri partecipanti hanno sottolineato la volontà e, insieme, la necessità, di incrementare la cooperazione internazionale

contro i crimini informatici, con il rafforzamento del *network* 24/7 e di quanto già esistente nei Paesi coinvolti nel vertice.
Ultime novità, inoltre, in *subiecta materia*, sono emerse in tempi recentissimi.
La prima concerne un accordo di cooperazione strategica, firmato dai direttori di ENISA (l'Agenzia europea per la sicurezza delle reti e dell'informazione) e di *Europol* in data 26 giugno 2014[168], presso la sede di *Europol*, all'Aja, volto a favorire una collaborazione più stretta e lo scambio di competenze nella lotta alla criminalità informatica.
In particolare, la collaborazione può comprendere: lo scambio di conoscenze e competenze specifiche, l'elaborazione di rapporti generali sulle condizioni correnti, resoconti basati su analisi strategiche e migliori pratiche, il potenziamento della formazione di capacità, con corsi e iniziative volte ad aumentare la consapevolezza per tutelare la sicurezza della rete e delle informazioni a livello dell'UE.
Ancora in data, 1 settembre 2014, è stata istituita da Europa e Stati Uniti una *task force*[169] battezzata *J-Cat* (*Joint Cybercrime ActionTaskforce*).
Ospitata presso il Centro criminalità informatica europea (EC3) di *Europol*[170], la *J-Cat* avrà il compito di coordinare le indagini internazionali e adottare misure contro le minacce del *cybercrime*. Italia, Austria, Germania, Francia, Olanda, Spagna, oltre a Usa e Canada fanno parte della struttura, che gode anche dell'appoggio di Australia e Colombia.
Coinvolta nelle indagini che comprendono più Paesi, *J-Cat* si

168 Testo integrale dell'accordo, reperibile sul sito www.enisa.europa.eu
169 Unità operativa costituita per singoli scopi o attività.
170 Sito www.europol.europa.eu

propone di aggiungere un valore significativo alla cooperazione giudiziaria internazionale, e massimizzare l'efficacia delle azioni congiunte e coordinate.

In un panorama normativo così diversificato e poco armonizzato, risulta difficile attuare una forma di cooperazione internazionale che non sia solo formale bensì reale.

Per combattere un fenomeno tanto capillare e globale come il crimine informatico, è necessario un legame più stretto tra gli Stati i quali, al di là dei particolarismi giuridici, devono volgere l'attenzione all'obiettivo comune della prevenzione e lotta al *cybercrime*.

CAPITOLO III

LA NORMATIVA SULLA *DATA RETENTION: PRIVACY* E SICUREZZA INFORMATICA

III.1 Premessa

L'interprete, dinanzi alle novità introdotte dalla l.18 marzo 2008, n.48, non può non porre la propria attenzione sugli interventi apportati dal legislatore, anche alla disciplina della conservazione dei dati di traffico per finalità di accertamento e repressione dei reati, prevista dall'art. 132 d.lgs. 30 giugno 2003, n.196 (il c.d. Codice della *privacy*).

L'enorme capacità di archiviazione dei supporti informatici su cui sono memorizzati i dati digitali e

l’assenza di barriere fisiche alla trasmissione degli stessi sui circuiti telematici, fanno si che i dati digitali pongano evidenti problemi di tutela della riservatezza individuale. Ed invero, tra gli aspetti più delicati in materia di indagini informatiche risiede l'individuazione di una disciplina che contemperi, da un lato, il fondamentale diritto di ogni cittadino alla protezione dei dati personali e, dall'altro, la necessità di utilizzare per finalità investigative i dati esterni di traffico[171].

Come si è potuto evincere, più volte, nel corso della presente trattazione, nell’ambito delle indagini digitali, non è raro che il diritto alla riservatezza subisca una compressione in occasione del cd. *tracing* (o “tracciamento”), espressione con cui si indica il “percorso a ritroso”, finalizzato a trovare l’origine della condotta di reato posta in essere con strumenti informatici, tramite l'individuazione e la conservazione di alcune informazioni “esterne”, legate alla comunicazione effettuata dall'utenza, similmente a quanto si verifica con i tabulati telefonici[172].

In tale contesto, le conflittualità con il diritto alla privacy sono dovute al fatto, che per accertare il traffico telematico, si conservano i *files di log* (o *files* di registro), che indicano le operazioni compiute dall’utente durante la navigazione e consentono, attraverso gli indirizzi IP (*Internet Protocol*), l’identificazione dello stesso, del destinatario e, a volte, la

171 L.LUPARIA, G.ZICCARDI, *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali,* Giuffrè, 2007, p.178 ss.

172 F.CAJANI, *Internet protocol. Questioni operative in tema di investigazioni penali e riservatezza,* in *Diritto dell'Internet,* 2008, p. 545.

ricostruzione del contenuto della comunicazione[173].

Per trovare un punto di equilibrio, tra gestione dei dati in questione, garanzie individuali e necessità investigative[174] appare quindi necessario determinare quali possano essere le informazioni concretamente archiviate, quali siano i soggetti gravati da tale obbligo e quale possa essere il tempo massimo di conservazione delle stesse.

III.2 Il difficile equilibrio tra *data retention e data protection.*

In questa prospettiva, giova soffermarsi sulla normativa interna concernente la *data retention*, sulla quale si è proceduto a molteplici modifiche in tempi piuttosto brevi.

La disciplina sulla conservazione dei dati esteriori di traffico, è stata introdotta nel nostro ordinamento giuridico con il d.lgs. 196/2003 (cd. Codice in materia di protezione dei dati personali o della *Privacy*), in seguito all'adozione della Direttiva 2002/58/CE[175], relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche.

Particolarmente importante è l'art. 132 del succitato decreto, che disciplina l'obbligo di "conservazione dei dati di traffico telefonico e telematico, a carico dei fornitori di servizi di comunicazione elettronica".

Questa disposizione è stata interessata da una sequela

173 F.CAJANI, *Alla ricerca del file (perduto),* in *Diritto dell'Internet,* 2006, p. 572 ss.

174 E.BASSOLI, *Acquisizione dei tabulati Vs. Privacy: la data retention al vaglio della Consulta,* in *Diritto dell'Internet,* 2007, p. 237.

175 Direttiva 2002/58/CE, in GUUE L 200/1, 31 luglio 2002

ravvicinata di interventi legislativi che hanno profondamente innovato la disciplina nel volgere di pochi anni.

L'oscillazione pendolare della legislazione tra istanze investigative e spinte protezionistiche della *privacy* ha risentito nello specifico del clima d'emergenza che ha contrassegnato le attività di terrorismo interno e soprattutto internazionale degli ultimi anni, nel cui ambito rileva in particolar modo il d.l. 27 luglio 2005, n. 144 (c.d. "decreto Pisanu" recante misure urgenti per il contrasto al terrorismo internazionale), convertito con modificazioni dalla l. 31 luglio 2005, n. 155[176].

Il decreto ha avuto il merito di colmare il vuoto legislativo presente nel testo dell'art. 132 comma 1, inserendovi sia l'obbligo di conservare i dati relativi al traffico telematico -con esclusione dei contenuti-[177] e le chiamate senza risposta, sia la possibilità di prorogare i tempi di conservazione, limitatamente alle fattispecie incriminatrici di maggiore gravità, indicate all'art. 407, comma 2, lett. a) c.p.p., e ai delitti commessi in danno ai sistemi informatici.

Proprio la possibilità di prorogare i tempi di conservazione nei "soli" casi di cui al comma sopracitato, garantisce per la Corte Costituzionale un bilanciamento tra principi confliggenti che si concretizza, nel verificare che l'opzione prescelta non segni un sacrificio manifestamente irregionevole del valore non reputato prevalente[178].

---

176 L.31 luglio 2005, n. 155, reperibile sul sito www.camera.it

177 L.A.D'ANGELO, *La conservazione dei dati del traffico telefonico e telematico tra esigenze investigative e tutela della privacy,* dal testo *Le nuove norme di contrasto al terrorismo,* (a cura di) A.A.Dalia, Giuffrè, 2006, p. 121 ss.

178 L. CORDI', *Diritto alla privacy ed acquisizione di tabulati telefonici: repressione e garanzia nel crocevia tra Consulta e legislatore,* in *Dir.*

Nello specifico con sentenza del 14 novembre 2006, n.372[179] la Corte Cost., ha ritenuto che la gravità dei delitti indicati dall'art. 407 comma 2 lett. *a* c.p.p., comporti "legittimamente" una compressione ulteriore alla *privacy,* la quale invece non sarebbe stata giustificata per la generalità dei reati.

È corretto, dunque, che si immolino le esigenze di riservatezza solo in presenza di taluni reati individuati secondo precise scelte di politica criminale.

Successivamente, in materia, sono intervenute la legge 48/2008; il decreto legislativo 30 maggio 2008, n. 109, attuativo della direttiva 2006/24/CE[180](c.d. Direttiva data retention o Frattini) relativa alla conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica, accessibili al pubblico o di reti pubbliche di comunicazione; nonché il d.l. 151/2008 convertito con l. 186/2008[181].

L'articolo 2 del decreto n. 109/2008 ha provveduto ad un'ampia riscrittura dell'art.132 del Codice della *privacy* che, era stato appunto a sua volta interpolato dalla l. 48/2008 con l'aggiunta dei commi 4-*ter* a 4-*quinquies.*

Questa materia, dunque, può essere definita come un vero e proprio "vortice" di modifiche, che ha determinato non poche incertezze negli operatori giudiziari e nei gestori

---

pen. e proc., 2007, p. 603

179 Nel caso di specie il G.i.p. del tribunale di Roma aveva sollevato questione di legittimità costituzionale dell'art. 132 del d.lgs. n.196/2003, nella parte in cui non prevedeva l'acquisizione dei dati per finalità di repressione dei reati non compresi nella previsione di cui all'art. 407 comma 2 lettera *a* c.p.p.

180 Direttiva 2006/24/CE, in GUUE L 105, 13 aprile 2006

181 S.ATERNO, A.CISTERNA, *Il legislatore interviene ancora sulla data retention, ma non è finita,* in *Dir. pen. e proc.,*2009, p. 286

telefonici.

L'articolo 1 del d.l 151/2008 contiene un riepilogo efficace delle problematiche che si sono addensate sin dai primi mesi del 2008 intorno alla disciplina della *data retention.*

La prima criticità proveniva dalla consapevolezza in base alla quale le norme, a prescindere da ogni tecnicismo, attraversano la vita di ogni cittadino e per profili non certo secondari.

Per la ragione menzionata poc'anzi, dovrebbe avere rilievo per ciascuno sapere per quanto tempo i dati del proprio traffico telefonico (fisso o mobile) e telematico sono conservate; se sia possibile o meno per l'autorità giudiziaria rintracciare i siti *internet* visitati o le pagine *web* consultate in un certo arco temporale.

La conservazione presso società private di miliardi di informazioni capaci di tracciare un profilo accurato di ogni persona titolare di un'utenza telefonica o telematica evoca, infatti, timori del tutto comprensibili.

Resta, infatti, costante l'esigenza di un giusto "oblio" sui contatti telefonici o sugli accessi telematici e ciò, non solo per quanto concerne la tutela della privacy, ma anche per il segmento che riguarda l'utilizzazione di tali dati ai fini investigativi[182].

Occorre ovviamente comporre secondo criteri ragionevoli i diritti dei singoli con la necessità di procedere, come recita il titolo del d.l n.151/2008, a un'efficace "prevenzione e accertamento di reati", attività rispetto alle quali l'acquisizione dei dati di traffico (art. 132 Codice della

182 S.ATERNO, A.CISTERNA, *Il legislatore interviene ancora sulla data retention, ma non è finita,* in *Dir. pen. e proc.,*2009, p. 285

privacy) costituisce spesso un provvedimento indispensabile.

La strada della ragionevolezza nell'individuazione di un termine per la *data retention* è, peraltro, imposta dalla circostanza che la distruzione eccessivamente rapida del dato di traffico rispetto al momento della sua generazione nei sistemi informatici degli operatori, danneggi irreparabilmente il diritto alla prova delle parti processuali con effetti sul piano delle garanzie costituzionali eccedenti la mera tutela della *privacy.*

Al fine di comprendere i punti di frizione tra la disciplina sulla conservazione dei dati telematici e la tutela del diritto alla privacy, bisogna *in primis,* chiarire l'oggetto dell'obbligo di conservazione e individuare i soggetti tenuti a rispettarlo, al fine di accertare, in specie, se l'identificazione dei siti visitati durante la navigazione rappresenti o meno un dato esteriore di traffico[183].

Il codice sulla protezione dei dati personali, non fornisce alcuna indicazione utile in tal senso.

Il decreto si limita a imporre al fornitore la conservazione dei dati relativi al traffico telematico, con l'esclusione del contenuto della comunicazione (art.132 comma 1) e definisce tali dati come "qualsiasi informazione sottoposta a trattamento per la trasmissione di una comunicazione su una rete di comunicazione elettronica" o per la "relativa fatturazione" (art. 4 comma 2 lett. h).

Queste disposizioni, però, non affrontano l'aspetto maggiormente discusso in tema di conservazione dei dati relativi al traffico telematico, ossia il fatto già menzionato,

183 G.ZICCARDI, *Privacy, sicurezza informatica, computer forensics e investigazioni digitali,* Giuffrè, 2012, p.142 ss.

che quest'ultimi consentano potenzialmente di tracciare gli accessi *internet*[184] (i dati I.P. di destinazione, dei *servers* consultati, da cui è desumibile l'indirizzo internet almeno delle *homepage* visualizzate) e i servizi utilizzati dall'utente (es. posta elettronica o *chat*).

Secondo parte della dottrina[185], con la custodia di tali informazioni, infatti, si ottiene un quadro molto chiaro e preciso dei movimenti effettuati in rete da ciascun abbonato, idoneo a ricostruire gusti, abitudini, preferenze di ogni tipo e, in definitiva, a rivelare anche notizie estranee alla commissione di illeciti penali e, come tali, vulneranti la tutela della riservatezza individuale.

Di conseguenza, gli indirizzi *I.P. destination* non dovrebbero essere custoditi.

Nell'intento di chiarire la portata delle disposizioni del Codice della privacy e di salvaguardare la riservatezza individuale, il 17 gennaio 2008[186], il Garante per la protezione dei dati personali, ha emesso un provvedimento sulla sicurezza dei dati di traffico telefonico e telematico, in cui ha introdotto alcune indicazioni contenute nella Direttiva 24/2006/CE.

In esso, l'Autorità ha imposto l'obbligo ai fornitori di servizi di comunicazione elettronica, la distruzione di una grande quantità di dati inerenti al traffico *on-line*, ritenuta in grado

184 G.VACIAGO, *La disciplina normativa sulla Data Retention e il ruolo degli internet service provider,* (a cura di) L.LUPARIA, *Internet provider e giustizia penale,* Giuffrè, 2012, p.140 ss.

185 M.VIGGIANO, *I dati personali nelle ricerche su internet,* in *Dir. inf. e informatica,* 2007, p. 379

186 Autorità Garante per la Protezione dei Dati personali, Provvedimento in tema di sicurezza dei dati di traffico telefonico e telematico, 17 gennaio 2008, reperibile sul sito www.garanteprivacy.it

di documentare il contenuto della navigazione del singolo utilizzatore della connessione.

Infatti, dopo aver circoscritto l'ambito soggettivo di applicazione della normativa ai soli fornitori, vale a dire ai soggetti che realizzano esclusivamente o prevalentemente una trasmissione di segnali su reti di comunicazioni elettroniche, con conseguente offerta indiscriminata di servizi a utenti finali (*Internet Service Provider* o ISP), il Garante si è preoccupato di circoscriverne l'ambito oggettivo.

In particolare, gli ISP sono tenuti a custodire, in distinti archivi, le informazioni che usano per la fatturazione e quelle di cui dispongono per la trasmissione delle comunicazioni, cancellando gli IP di destinazione e le pagine web (o URL) visitate, e creare apposite soluzioni informatiche, idonee ad assicurare il controllo delle attività svolte sui dati di traffico da ciascun incaricato del trattamento.

In questo quadro, così posto, il provvedimento non impone alcun dovere di conservazione in capo, ad esempio, ai gestori dei motori di ricerca e dei contenuti dei siti *web* in *internet* (cc.dd. *content provider*)[187], ai gestori di esercizi pubblici come gli *internet point* e agli *internet café,* oppure alle organizzazioni sia pubbliche sia private che dotino il proprio personale di postazioni connesse a reti informatiche e

187 Essi, in particolare, devono conservare esclusivamente i dati di traffico telematico funzionali alla fornitura e alla fatturazione del servizio di connessione e non i dati di traffico apparentemente "esterni" alla comunicazione (es. pagine web visitate o indirizzi IP di destinazione), poiché essi, possono coincidere di fatto con il "contenuto" della comunicazione, consentendo di ricostruire relazioni personali, convinzioni religiose, orientamenti politici, abitudini sessuali e stato di salute(art. 3). Garante della *privacy, Relazione 2008, Garanzia e sicurezza dei dati: l'attività dell'Autorità*, in *www.garanteprivacy.it*

telefoniche non accessibili al pubblico.

Pertanto, dalla lettura combinata delle norme del d.lgs. 196/2003, del d.lgs. 109/2008 e delle prescrizioni emanate dal Garante della privacy, si deve concludere che l'IP di destinazione e i siti visionati sono, di fatto, esclusi dagli obblighi di conservazione, così da dover essere immediatamente cancellati.

Il fatto di limitare tali obblighi di conservazione ai soli IP di accesso, però, potrebbe costituire un grave limite nello svolgimento delle investigazioni digitali di polizia, con la conseguenza, in molti casi, di determinare l'impossibilità di identificare l'utente, e questo potrebbe finanche compromettere lo stesso diritto di difesa dall'indagato che voglia dimostrare la propria innocenza in base a prove informatiche (ad es. Alibi informatico[188]), o della persona offesa, che voglia fornire una prova informatica a riscontro di quanto esposto in denuncia[189].

A ben vedere, appunto, i dati telematici detenuti dagli *internet providers,* ossia dai fornitori *ex* art. 132 comma 1 d.lgs. 196/2003, sono costituiti da informazioni per lo più relative alle registrazioni degli accessi (c.d. *files di log* degli indirizzi IP) e, come tali, assimilabili a quelle di telefonia, in quanto individuano il dispositivo elettronico (di norma *un computer)* che si è connesso alla rete e indicano l'associazione tra indirizzo IP assegnato all'utente e numero telefonico chiamato.

Non dovrebbero, quindi, sussistere in linea di principio gravi

188 V. infra cap.2, par. II.6.

189S.ATERNO,A.CISTERNA, *Il legislatore interviene ancora sulla data retention, ma non è finita,* in *Dir. pen.e proc.,* 2009, p. 279

violazioni della *privacy* individuale nell'acquisizione di tali dati, anche se comprensivi di IP di destinazione[190].

Per quanto concerne, infine, i termini di conservazione del traffico telematico, l'art. 132 d. lgs. 196/2003 ne prevede una archiviazione temporanea finalizzata in via esclusiva all'accertamento e alla repressione dei reati.

Inizialmente, il decreto Pisanu, ha introdotto diversi termini di conservazione in base al tipo di dato archiviato (telefonico, telematico o chiamata senza risposta), stabilendone l'acquisizione con decreto motivato del P.M.

Le leggi di riforma adottate nel 2008, poi, hanno riproposto sia la possibilità di acquisire le informazioni relative al traffico tramite decreto dell'organo inquirente, sia la differenziazione dei periodi di conservazione, in base al tipo di informazione conservata a prescindere dalla gravità del reato perseguito[191].

Sicché, attualmente, si ha un termine massimo pari a ventiquattro mesi per il traffico telefonico, a dodici mesi per quello telematico e a trenta giorni per i dati relativi alle chiamate senza risposta.

Simile distinzione temporale, che prevede un periodo di archiviazione più limitato per i dati di traffico telematico non è, invero, richiesta dalla direttiva comunitaria 2006/24/CE e non sembra trovare la sua ragion d'essere nella necessità di tutelare, maggiormente, la vita privata individuale con riferimento all'uso di tali dati.

---

190 S.ATERNO, F.CAJANI, *La disciplina in tema di conservazione dei dati,* in *Computer forensics e indagini digitali,* Experta, 2011, p. 249

191 G.VACIAGO, *La disciplina normativa sulla Data Retention e il ruolo degli internet service provider,* (a cura di) L.LUPARIA, *Internet provider e giustizia penale,* Giuffrè, 2012, p.145 ss.

Infatti, come i dati relativi al traffico telefonico, i dati concernenti il traffico telematico archiviati, si limitano per espressa previsione normativa, ai soli contenuti esterni della comunicazione (art. 132, comma 1, d.lgs. 196/2003).

Sotto questo profilo, allora, sarebbe stato preferibile introdurre dei termini di conservazione omogenei sia per i dati telefonici che per quelli telematici, con previsione, semmai, di tempi di archiviazione più lunghi[192] per i reati di maggiore gravità.

Le modalità di conservazione dei dati in discorso presso i soggetti privati, sono regolamentate dalla disposizioni adottate dal Garante della Privacy, che ha il compito di individuare le misure adeguate a garantire i diritti individuali (es. sistemi di cifratura) e di controllarne l'applicazione.

Tali presidi a garanzia della riservatezza avrebbero dovuto essere adottati dagli *internet providers* entro il 30 giugno 2009, ma gli elevati costi dell'operazione hanno reso difficoltoso, nei fatti, il rispetto della normativa, nonostante l'obbligatorietà della disciplina e le pesanti sanzioni comminate in caso di inadempimento[193].

Pertanto, sotto questo profilo, la protezione dei dati personali e la loro stessa genuinità risultano essere esposte a un concreto pericolo di lesione.

Inoltre, emerge un ulteriore aspetto di criticità in relazione alla procedura di cancellazione o di riduzione ad anonimato dei dati, una volta trascorso il termine massimo di

---

192 L'art. 6, della Direttiva 2006/24/CE, ammette che il termine per la conservazione dei dati esterni di comunicazioni telefoniche e telematiche, possa essere stabilito fino a un massimo di 24 mesi

193 S.ATERNO, F.CAJANI, *La disciplina in tema di conservazione dei dati,* in *Computer forensics e indagini digitali,* Experta, 2011, p. 252

conservazione degli stessi: manca, infatti, la previsione di una procedura standardizzata che provi, ad esempio con verbali, l'effettivo e corretto svolgimento delle operazioni necessarie.

III.2.1 **L'ipotesi speciale: la conservazione preventiva dei dati informatici ai fini investigativi.**

Molto più invasiva del diritto alla riservatezza personale rispetto a quanto sinora esposto pare essere, invece, l'ipotesi speciale di conservazione dei dati telematici a seguito di attività di investigazione preventiva penale, introdotta all'art. 132, comma 4-*ter* d. lgs. 196/2003 dalla legge 48/2008 (c.d. congelamento dei dati telematici).

Si tratta di un'attività di carattere eccezionale ed urgente (in ambito internazionale e non), rimessa all'iniziativa della polizia giudiziaria, che può essere svolta preventivamente e, quindi, anche in assenza di una *notitia criminis*, finalizzata alla conservazione e protezione di dati relativi al traffico telematico, per un periodo di novanta giorni prorogabile fino a sei mesi[194].

Questa attività di "congelamento" (cd. *freezing*) di dati telematici, si differenzia dall'ipotesi di conservazione dati disciplinata al primo comma, in quanto è rivolta, oltre che ai fornitori di rete, a tutti i soggetti che offrono direttamente o indirettamente servizi di comunicazione elettronica, i gestori di siti *internet* che diffondono contenuti sulla rete (c.d.

194 C.FATTA, *La tutela della privacy alla prova dell'obbligo di data retention e delle misure antiterrorismo,* in *Dir. dell'inf. e dell'inform., 2008,* p. 395 ss.

content provider) ed i gestori dei motori di ricerca.

I dati di traffico telematico trattati da queste ultime due categorie di soggetti, in particolare, sono equiparabili al contenuto della comunicazione, perché consentono di ripercorrere facilmente tutte le operazioni compiute dall'utente *on line* anche all'interno del singolo sito.

Tali informazioni, quindi, non possono essere considerate meri "dati esterni", poiché essi riguardano precisamente il servizi forniti dai *provider* e spesso consentono di risalire all'oggetto della comunicazione[195].

Il c.d. "congelamento" dei dati telematici, previsto all'art. 132 comma 4*ter,* è finalizzato espressamente allo svolgimento delle indagini pre-procedimentali, con conseguente inutilizzabilità, nel procedimento penale vero e proprio, *ex* art. 226 comma 5 disp. att. c.p.p.

Questa formula aperta consente alla polizia giudiziaria di ricorrere allo strumento *de quo* per qualunque tipo di reato, anche laddove le finalità di giustizia non giustifichino la compressione del diritto alla riservatezza.

Sarebbe preferibile, in un ottica di maggior rispetto della riservatezza individuale, stabilire più rigorose condizioni di ammissibilità per lo svolgimento di tale attività d'indagine.

195 F.CERQUA, *Il difficile equilibrio tra la protezione dei dati personali e le indagini informatiche,* in *Sistema Penale e criminalità informatica,*(a cura di) L.LUPARIA, Giuffrè, 2009, p. 236.

III.2.2 **La normativa sulla *data retention* la Corte di Giustizia dell'Unione europea la dichiara invalida.**

In data 8 aprile 2014, la direttiva 2006/24/EU sulla *data retention,* è stata dichiarata invalida dalla Corte di Giustizia dell'Unione europea[196].

Già nel marzo 2010 la Corte costituzionale tedesca, aveva dichiarato l'incostituzionalità della legge sull'archiviazione di massa di dati telefonici e di navigazione su *internet,* derivante dall'implementazione della direttiva.

La Corte aveva sostenuto che tale normativa violava la segretezza della comunicazioni, archiviava dati sensibili in mancanza di parametri di sicurezza per i cittadini ed era carente di informazioni precise in merito a come i dati fossero utilizzati[197].

Ciò premesso non è difficile intuire quali sono i motivi che hanno indotto i giudici europei a dichiarare l'invalidità della direttiva.

Nello specifico, infatti, questi ultimi hanno rinvenuto in essa un evidente contrasto con il principio di proporzionalità, letto e considerato alla luce degli artt. 7, 8 e 52, par.1, della Carta dei diritti fondamentali dell'Unione europea[198].

La Corte è giunta a tale storica decisione poiché investita *ex* art. 267, lett.*b*) TFUE, del vaglio di una serie di questioni pregiudiziali, sollevate nelle cause riunite C-293/12 (Digital

196Testo della sentenza n. 54/2014, reperibile sul sito www.garanteprivacy.it, doc-web n. 3043486.

197 *Bundesverfassungsgericht,* sent. 2 marzo 2010, n. 256/2008, reperibile su sito www.bverfg.de

198 E.COLOMBO, *Data retention e Corte di Giustizia: riflessioni a prima lettura sulla declaratoria di invalidità della direttiva 2006/26/CE,* in *Cass. Pen.,* 2014, p. 2705 ss.

Rights Ltd) e C-594/12 (Karntner Landesregierung)[199].

In breve, nella causa C-293/12, la ricorrente (*Digital Rights Ireland Ltd* - DRI), società volta alla promozione ed alla protezione dei diritti civili e dei diritti dell'uomo, in particolare nel contesto delle moderne tecnologie di comunicazione, aveva presentato un ricorso dinanzi la *High Court* contro due ministri del governo irlandese, il comandante della polizia irlandese, l'Irlanda e l'*Attorney General* dello Stato irlandese, riguardante la legittimità delle misure legislative e amministrative irlandesi sulla conservazione dei dati relativi alle comunicazioni elettroniche, con la richiesta di annullamento dei provvedimenti in base ai quali i fornitori di servizi di telecomunicazioni, erano tenuti a conservare i dati, in quanto ritenuti incompatibili con la Costituzione irlandese e con il diritto dell'Unione.

Si pose, dunque, la questione di legittimità della stessa direttiva 2006/24 rispetto alle previsioni della Carta e della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali.

Nella seconda causa C-594/12, il sig. *Seitlinger* presentò dinanzi al *Verfassungsgerichtshof* austriaco un ricorso molto somigliante al precedente, fondato sull'art. 140, par. 1, del *Bundes-Verfassungsgesetz* (B-VG), con il quale contestava l'incostituzionalità dell'art. 102 *bis* del *Telekommunikationsgesetz* del 2003 (TKG), nella misura in cui consente ai fornitori di servizio di conservare dati di traffico e telematico, in maniera piuttosto ampia, in relazione

199 Le cause riunite C-293/12 e C-594/12, sono reperibili sul sito www.curia.europa.eu

ad un numero illimitato di soggetti e per un tempo abbastanza lungo[200].

A tal proposito, la Corte costituzionale austriaca ha anche espresso il proprio avviso sulla questione, secondo il quale la conservazione di un tale quantitativo di dati, finirebbe col riguardare quasi esclusivamente soggetti la cui condotta non giustificherebbe la conservazione di dati nei loro confronti. Secondo la Corte costituzionale austriaca, infatti, vi sarebbero dei forti dubbi sull'idoneità della direttiva 2006/24 a raggiungere gli obiettivi che intende perseguire e, sulla proporzionalità della sua ingerenza nei confronti dei diritti fondamentali, in particolare quelli previsti dagli artt. 7,8 e 11 della Carta dei diritti fondamentali dell'UE.

Come già accennato, la Corte di giustizia, ai fini della trattazione orale della causa e della sua pronuncia finale, ha deciso di riunire i due rinvii pregiudiziali, in quanto entrambi riconducibili nella sostanza ad una richiesta di esame sulla validità della direttiva 2006/24/CE, alla luce della sua compatibilità con gli articoli di cui *supra*.

Nella trattazione di tale causa, la Corte di giustizia ha affermato[201], in primo luogo, che la conservazione dei dati, costituisce *prima facie* un'ingerenza nei diritti fondamentali dei soggetti coinvolti, in quanto la conservazione di tali dati è in grado di condurre a delle conclusioni ben precise riguardo le vite private delle persone i cui dati sono stati trattenuti, quali abitudini quotidiane, luoghi di residenza permanente o

200 R.FLOR, *La Corte di Giustizia considera la direttiva europea 2006/24 sulla c.d."data retention" contraria ai diritti fondamentali. Una lunga storia a lieto fine?,* in *www.penalecontemporaneo.it*

201 *Conservazione dei dati telefonici e telematici: invalida la direttiva europea,* reperibile sul sito www.altalex.it.

temporanea, trasferimenti quotidiani o di altra natura, attività condotte, relazioni sociali e ambienti sociali frequentati (punto 27 della sentenza).

Infatti, sebbene gli articoli 1(2) e 5(2), della direttiva 2006/24 sanciscano il divieto di conservazione del contenuto delle comunicazioni o delle informazioni consultate attraverso l'uso di una rete di comunicazioni elettroniche, vi è una contraddizione, laddove la stessa autorizza la conservazione di quei dati ritenuti necessari a tracciare e determinare: la fonte e la destinazione di una comunicazione; la data, l'ora, la durata e il tipo di comunicazione; le attrezzature di comunicazione degli utenti; e, l'ubicazione delle apparecchiature di comunicazione mobile[202].

Quanto detto permetterebbe, comunque, di identificare il nome e l'indirizzo dell'abbonato o dell'utente registrato, i numeri di telefono coinvolti e l'indirizzo IP della connessione internet,di conseguenza, la conservazione di tali dati e, soprattutto, il possibile accesso ad essi da parte delle autorità nazionali competenti, inciderebbe direttamente e specificamente sulla vita privata dei soggetti coinvolti, quindi sui diritti garantiti dall'articolo 7 della Carta dei diritti fondamentali dell'UE.

Inoltre, anche se la direttiva non consente di archiviare i dati relativi ai contenuti delle comunicazioni, le sue previsioni hanno comunque un effetto sul possibile utilizzo dei mezzi di comunicazione da parte degli utenti e sull'esercizio della loro libertà di espressione (ex art. 11 della Carta), nonché

202 A.RODOLFI, *Il regime normativo della data retention nell'ordinamento italiano. Stato attuale e problematiche concrete,* in *Ciberspazio e diritto, 2010,* p. 148 ss.

permettono un possibile controllo *ex post* delle attività personali e professionali dei cittadini europei che, seppur appunto esercitato a posteriori in occasione dell'impiego delle informazioni, minaccia in modo permanente e per tutto il periodo della loro conservazione, il diritto alla riservatezza.
Sulla base di quanto precede, la Corte di giustizia ha così affermato che gli obblighi imposti dalla direttiva 2006/24 sui fornitori di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione, di conservare, per un certo periodo di tempo, i dati relativi alla vita privata di una persona e le sue comunicazioni, costituisce un'ingerenza in sé nei diritti garantiti dall'articolo 7 della Carta dei diritti fondamentali dell'UE[203].
Allo stesso modo, la possibilità per le autorità nazionali competenti di accedere a tali dati, precedentemente conservati, costituisce una violazione non solo dei diritti garantiti dall'articolo 7 della Carta, ma anche del diritto fondamentale alla protezione dei dati personali, ai sensi dell'articolo 8 della Carta stessa, in quanto l'accesso a tali dati comporta il loro trattamento da parte delle autorità nazionali competenti.
Secondo la Corte di giustizia, quindi, l'ingerenza delle misure della direttiva 2006/24 nei confronti dei diritti fondamentali, di cui agli articoli 7-8 della Carta dei diritti fondamentali dell'UE sarebbe particolarmente grave.
Infatti, poiché i dati sono conservati e successivamente utilizzati senza che l'abbonato o l'utente registrato sia

203 F.CERQUA, *La Corte di Giustizia dichiara invalida la direttiva sulla Data retention: brevi osservazioni,* reperibile sul sito www.dirittopenaleeuropeo.it

informato al riguardo, è molto probabile che generino nella persona in questione la sensazione di essere costantemente sorvegliata.

III.2.3 **L' evidente contrasto della direttiva 2006/24 con "il principio di proporzionalità"**

La Corte di giustizia, dopo aver constatato l'ingerenza delle misure previste dalla direttiva in oggetto nei confronti dei diritti fondamentali delle persone coinvolte, ha ritenuto opportuno verificare se tali ingerenze potessero essere giustificate ai sensi dell'articolo 52 della Carta dei diritti fondamentali dell'UE, il cui paragrafo 1 dispone che: "Eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta, devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni, solo laddove siano necessarie e rispondano effettivamente, a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui"[204].

La Corte ha ammesso che le tecnologie informatiche e i mezzi di comunicazione elettronica possono essere estremamente utili nell'ambito delle attività di indagine, permettendo alle autorità nazionali di avere maggiori opportunità nella lotta alla criminalità grave.

---

204 R.FLOR, *La Corte di Giustizia considera la direttiva europea 2006/24 sulla c.d."data retention" contraria ai diritti fondamentali. Una lunga storia a lieto fine?,* in www.penalecontemporaneo.it

In questo senso, gli obblighi di conservazione dei dati, dovrebbero essere considerati appropriati al raggiungimento degli obiettivi perseguiti dalla direttiva europea.

La Corte, però, ha anche evidenziato che il rispetto della vita privata richiede che le deroghe e i limiti relativi alla protezione dei dati personali debbano essere applicati solo ed esclusivamente in casi di stretta necessità.

Anche se la lotta contro gravi crimini risulta essere essenziale per assicurare la sicurezza pubblica e, la sua efficacia può dipendere da un largo uso di moderne tecniche investigative, la "necessità" di archiviare i dati di traffico per il raggiungimento di un "interesse generale", seppur di notevole rilievo, non è di per sé giustificata[205].

Il legislatore europeo, avrebbe dovuto imporre chiare e precise regole relative all'applicazione della *data retention,* tramite l'introduzione, secondo i Giudici, di standard minimi di garanzia per assicurare al cittadino europeo, o alla persona i cui dati sono archiviati, una effettiva protezione contro i rischi di abusi o di accesso illegale alle informazioni, soprattutto in casi come quello in esame, in cui il trattamento dei dati avviene in modo automatizzato ed è intrinsecamente "pericoloso".

Sulla compressione dei diritti fondamentali, causati dalla direttiva, la Corte è giunta alle seguenti conclusioni:

- L'ingerenza è particolarmente ampia, poiché la direttiva comprende tutti i dati relativi al traffico

205 L.BENEDIZIONE, E.PARIS, *Bilanciamento e dialogo fra le Corti nell'Unione europea: la Corte di Giustizia dichiara invalida la Data Retention directiva,* reperibile sul sito www.diritticomparati.it

riguardante tutti i mezzi di comunicazione elettronica, senza alcuna distinzione, limitazione o eccezione a seconda dell'obiettivo di lotta contro i reati gravi.

- Inoltre, la direttiva non prevede alcun criterio oggettivo che permetta di delimitare l'accesso delle autorità nazionali competenti ai dati e il loro uso ulteriore a fini di prevenzione, non contiene cioè le condizioni sostanziali e procedurali ad esso relative.

- Per di più, per quel che riguarda le norme sulla protezione e sulla sicurezza dei dati conservati dai *providers,* l'art. 7 della direttiva non garantisce che sia applicato da detti fornitori un livello particolarmente elevato di protezione e di sicurezza, attraverso misure tecniche e organizzative, ma li autorizza a tener conto di considerazioni economiche nel determinare il livello di sicurezza da essi applicato. Ed ancora più grave, "tale direttiva non impone che i dati di cui trattasi siano conservati sul territorio dell'Unione e, di conseguenza, non si può ritenere pienamente garantito il controllo da parte di un'autorità indipendente esplicitamente richiesto dall'art. 8, par.3, della Carta.

- Infine, l'art. 6 della direttiva 2006/24 imponeva la conservazione dei dati non per un periodo preciso e comune a tutti gli Stati, ma valutabile tra un minimo di 6 mesi ed un massimo di 24 mesi, senza distinzione

tra le categorie di dati a seconda della loro eventuale utilità ai fini dell'obiettivo perseguito o a seconda delle persone interessate. Sotto questo profilo, la direttiva è stata così recepita in modo non uniforme dagli Stati, evidenziando quindi il fallimento dell'obiettivo di armonizzazione della stessa.

Per tutte queste ragioni, la Corte ha invalidato la direttiva 2006/24, in quanto incompatibile con i limiti imposti dal principio di proporzionalità, alla luce dei degli art. 7-8 e 11, contenuti nella Carta dei diritti fondamentali dell'UE.

111.2.4 **Prospettive future**

Con la sentenza sulla c.d. *data retention*, la Corte di Giustizia ha invalidato la direttiva 2006/24, aprendo nuovi scenari sia a livello europeo che a livello nazionale[206].

Il dato positivo risiede nel fatto che la Corte ha indicato al legislatore europeo, la strada da percorrere per garantire i diritti fondamentali dell'individuo, pur non imponendo la rinuncia *in toto* agli strumenti tecnologici indispensabili per la prevenzione e la repressione di gravi reati.

L'aspetto negativo, invece, risiede nel fatto che molti paesi europei, compresa l'Italia, si trovano a dover affrontare immediatamente la delicata questione della permanente "validità" delle rispettive norme nazionali di attuazione della

206 G.VACIAGO, *La Corte di Giustizia invalida la direttiva 2006/24/EU sulla data retention,* reperibile sul sito www.diritto24.ilsole24ore.com

direttiva, sulla base delle quali vengono svolte importanti attività investigative per l'accertamento e la prevenzione dei crimini.

La decisione della Corte di Giustizia, infatti, non determina l'invalidità delle normative nazionali in tema di conservazione dei dati da parte degli Stati Membri, in quanto ai sensi dell'art. 267 del Trattato sul funzionamento dell'Unione Europea, la competenza della Corte può avere efficacia diretta solo sugli atti comunitari, ma non su quelli nazionali.

In Inghilterra, ad esempio, il governo si è affrettato a confermare verso gli operatori di telecomunicazioni, che la legge non è abrogata e che il vincolo della conservazione rimane.

La decisione della Corte europea di dichiarare l'invalidità della direttiva lascia aperti molti interrogativi.

Le soluzioni proponibili potrebbero rinvenirsi proprio nelle linee guida, inizialmente menzionate, che la Corte di giustizia sembra aver voluto fornire al legislatore dell'UE.

In primo luogo restringere e armonizzare le finalità della *data retention* e le tipologie di reati in forza dei quali si può accedere e utilizzare i dati di traffico; assicurare una maggiore uniformità a livello europeo dei periodi di conservazione dei dati; limitare il numero dei soggetti autorizzati ad accedere a tali dati e ridurre le categorie dei dati da conservare, infine, valutare come i rilievi sulla trasferibilità dei dati personali al di fuori del territorio UE abbiano delle implicazioni non secondarie, vista la possibilità, ai sensi della direttiva annullata, di trasferire gli

stessi dati da autorità dell' UE ad entità extra-UE[207].

Sono questi i rilievi da cui partire per predisporre una futura riforma sulla *data retention.*

III.3 La decisione della Corte Costituzionale tedesca sulla: Online Durchsuchung

Il 27 febbraio 2008, la Corte Costituzionale Federale tedesca (*Bundesverfassungsgericht*) per la prima volta ha riconosciuto, con una storica decisione sulla c.d. *Online Durchsuchung*[208], un nuovo diritto costituzionale alla "riservatezza ed integrità dei sistemi tecnologici d'informazione".

La questione che la Corte ha dovuto affrontare è stata la costituzionalità della legge sulla protezione della Costituzione del *North Rein-Westfalia,* al paragrafo 5 co. 2°, in materia di raccolta e trattamento dei dati degli utenti, in specie, da sistemi informatici ed attraverso la rete[209].

In particolare, la legge sopracitata, autorizzava un organismo di *intelligence*[210], a "protezione della Costituzione", ad

207 R.FLOR, *La Corte di Giustizia considera la direttiva europea 2006/24 sulla c.d."data retention" contraria ai diritti fondamentali. Una lunga storia a lieto fine?,* in www.penalecontemporaneo.it

208 BVerfG 370/07 –595/07, 27.2.2008, reperibile sul sito www.bverfg.de

209 R. FLOR, *Investigazioni ad alto contenuto tecnologico e tutela dei diritti fondamentali della persona nella recente giurisprudenza del Bundesverfassungsgerich: la decisione del 27 febbraio 2008 sulla Online Durchsuchung e la sua portata alla luce della sentenza 2 marzo 2010 data retention,* in *Ciberspazio e diritto*, 2010, p. 360

210 Si tratta di un organismo afferente al Ministero dell'Interno, che ha il compito di raccogliere ed analizzare anche le informazioni personali, notizie e documentazione, fra gli altri, su fenomeni criminosi contro la libertà e l'ordine democratico, nonché la sicurezza della Federazione o di un *Land,* volti all'interferenza illecita degli organi costituzionali della Federazione; ovvero atti riferiti all'uso della forza o atti preparatori di fronte

effettuare due tipi di misure d'indagine: in primo luogo, il monitoraggio e la ricognizione segreti di *Internet* e, in secondo luogo, l'accesso segreto a sistemi informatici.

Il monitoraggio segreto di *Internet* è una misura con cui l'Agenzia di protezione della Costituzione, ottiene informazioni sul contenuto di comunicazioni via *Internet* tramite l'uso di tecnologie come l'accesso ad un sito aperto, la partecipazione a *chat* o *forum online*, ma anche l'accesso a siti privati utilizzando una *password* ottenuta altrove, per esempio tramite un informatore.

Al contrario, l'accesso segreto ad un sistema tecnologico d'informazione, è considerato un'infiltrazione tecnica, che può avvenire sfruttando falle nelle misure di sicurezza del sistema-bersaglio o tramite l'installazione di programmi-spia.

Secondo la Corte, qualsiasi legge che permetta attività simili, deve essere in grado di dimostrare che tale intervento sia giustificato dalla protezione di altri diritti costituzionali, che lo stesso sia necessario per assicurare tale protezione e che sia proporzionato nel suo impatto.

La Corte medesima, però, ha giudicato la legge non conforme alla Costituzione e per tale ragione ne ha dichiarato l' illegittimità.

Il ragionamento della Corte e la portata della decisione furono una sorpresa per molti osservatori, soprattutto dinanzi alla scelta della stessa di formulare un nuovo diritto fondamentale che proteggesse esplicitamente il diritto di

---

ad un pericolo per gli affari esteri della Germania.

privacy e i diritti personali dei cittadini nelle tecnologie dell'informazione e comunicazione (ICT).

A questo punto, è importante fare una premessa.

L'emendamento al paragrafo 5 co. 2 oggetto di questa decisione, era solo un aspetto della discussione a livello federale, riguardo la centralità di un nuovo metodo d'investigazione, ossia la ricerca a distanza di computer e portatili.

È quindi necessario tenere in conto questo precedente dibattito.

Il dibattito pubblico e giuridico su questo argomento si scatenò nel 2006, a partire da una richiesta operata da un procuratore statale alla Corte Federale di giustizia tedesca (Bundesgerichtshof, BGH).

In questa domanda il procuratore chiese un mandato per poter effettuare ricerche a distanza in *computer* sospetti nell'ambito di una investigazione sul terrorismo, attraverso l'installazione occulta di un programma di sorveglianza simile ad un *Trojan*[211].

La richiesta venne rigettata il 25 novembre 2006.

Il procuratore statale, però, propose appello riferendosi agli artt. 94, 102 e 110 del codice penale, i quali consentivano questo genere di ricerche.

Nella sua argomentazione si effettuava un parallelismo fra la ricerca fisica dei luoghi, regolata da questi articoli, e l'accesso a distanza in un *computer* di un sospettato.

211 Un Trojan in ambito informatico indica un tipo di virus che di solito si cela all'interno di un programma innocuo.

Ma la BGH non condivise, infatti rigettò nel suo giudizio, l'analogia tra una ricerca tradizionale di luoghi fisici e ricerche clandestine su *computer* e dispose che, senza un'esplicita regolamentazione, garantire una tale richiesta di autorizzazione sarebbe stato un atto *ultra vires*.

La decisione, però, lasciò intendere che regolamentazioni appropriate avrebbero potuto essere introdotte per creare questa nuova ricerca e nuovi poteri di confisca ed, infatti, in seguito venne emendata la legge regionale dello Stato del Nord Reno-Westfalia "per la protezione della Costituzione", introducendo di fatto tale potere "di diritto".

La legge disponeva, appunto, il diritto per l'Agenzia di protezione della Costituzione e i principali servizi segreti della Germania per gli affari internazionali di acquisire informazioni e dati direttamente dai sospettati.
Il metodo alla base ossia l'infiltrazione in un *computer* attraverso mezzi tecnici, riferito anche alla "ricerca *online*", *"Trojan* federali", o "ricerca a distanza", è una forma specifica di raccolta di informazioni.
Tali attività investigative erano in grado di risolvere quelle difficoltà che nelle investigazioni emergono se criminali, in particolare gruppi terroristici, usano *Internet* per comunicazioni e per pianificare e commettere crimini.
Lo scopo di setacciare un *computer* a distanza, è quello di abilitare gli investigatori a cercare dei dati immagazzinati nell'*hard disk* e sulla memoria attiva del *computer,* intercettare il traffico di posta elettronica e controllare le abitudini di navigazione web e la messaggistica istantanea.
Per raggiungere tale scopo, un programma appositamente

progettato, uno strumento "*remote forensic software"* (RFS), viene posto sul computer del sospettato senza che egli ne sia a conoscenza.

Il programma è quindi in grado di copiare tutti i dati sul computer e successivamente trasferirli ai fini della valutazione. Un software di questo tipo condivide caratteristiche cruciali con dei *malware* ben conosciuti, come il già citato *Trojan*.

Questi *malware,* in particolare possono essere usati per accedere al sistema-bersaglio ed estrarne dati personali, dunque sono adatti anche per la raccolta di dati da parte della polizia.

Questo è il motivo per il quale l'RFS ,che facilita la ricerca a distanza, in Germania viene spesso chiamato "*Trojan* federale".

Il vantaggio nell'usare dette tecnologie è che possono essere installate clandestinamente, senza entrare in casa del sospettato o in luoghi fisici.

Gli strumenti RFS sono progettati per essere "camuffati" come programmi innocui, al contrario, invece, contengono un codice pericoloso e maligno in grado di ingannare il sospettato con l'obiettivo di indurlo ad installare il *software*.

Quindi, come le loro controparti criminali, i *Trojan* della polizia richiedono la cooperazione ingenua del bersaglio, il che risulta facilmente realizzabile se si pensa che basta aprire un'*e-mail,* per esempio un messaggio che si presume venire da una agenzia statale in buona fede, come il Consiglio locale o il Dipartimento delle pensioni.

Se l'infiltrazione riesce, questo metodo offre vantaggi

considerevoli all'autorità investigativa, rispetto ai metodi di investigazione tradizionali.

Poiché tale metodo viene utilizzato all'insaputa del sospettato, costui non è allarmato dal fatto che la polizia lo consideri un obiettivo, in contrapposizione ad una tradizionale perquisizione in casa.

Inoltre, il sistema consente la raccolta di dati criptati in forma decriptata, potendo l'autorità investigativa accedervi nello stesso momento in cui l'utente li digita.

In aggiunta, possono essere raccolte *password* ed ulteriori informazioni sul modo di utilizzo del computer da parte del sospettato.

Questo tipo di informazioni sarebbero difficili da ottenere tramite l'utilizzo di metodi investigativi tradizionali.

Un ricorso costituzionale è ammesso dalla legge tedesca, solo se il ricorrente è in grado di provare di aver subito una violazione dei diritti fondamentali elencati nella prima parte della Costituzione.

L'emendamento del paragrafo 5.2 della legge sulla protezione della Costituzione del Nord Reno-*Westfalia* limita l'applicabilità di tale norma ad attività illegali "che minacciano il libero ordine fondamentale democratico o la sicurezza della Federazione o di uno Stato Federale" e durante la discussione riguardo l'introduzione della ricerca online come misura investigativa a livello federale, è stato stabilito che tale mezzo potrebbe essere usato solo per indagare su sospettati in investigazioni sul terrorismo o casi comparabilmente gravi.

Ciononostante, furono quattro i ricorrenti che proposero

ricorso costituzionale contro l'emendamento del paragrafo 5.2, affermando che la norma costituiva una violazione diretta dei loro diritti costituzionali, anche se nessuno dei ricorrenti era stato coinvolto in indagini penali.

La Corte accettò questo punto di vista ed ammise i loro ricorsi.

I quattro ricorrenti dimostrarono che, sebbene non coinvolti loro stessi in alcun comportamento illecito, le loro attività professionali avrebbero potuto essere erroneamente sottoposte ad indagine, con la conseguenza di causare la perquisizione a distanza dei loro *pc,* in ragione del nuovo emendamento, con violazione dei loro diritti costituzionalmente garantiti.

Difatti, uno di loro era un giornalista che per motivi di lavoro accedeva a siti *Internet* gestiti da estremisti in connessione con organizzazioni eversive e partecipava a *chat* ospitate in tali siti web al contempo, inoltre, usava il *computer* per motivi privati.

Un altro ricorrente era un membro di un partito politico sotto l'osservazione dell'Agenzia per la protezione della Costituzione del Nord Reno-*Westfalia*, che utilizzava il computer sia per motivi di lavoro che per uso personale.

Un ulteriore ricorrente era un avvocato che assisteva i richiedenti asilo, alcuni dei quali erano sotto il controllo dell'Autorità per la protezione della Costituzione del Nord Reno-Westfalia e, anch'esso, usava il computer allo stesso tempo per scopi di lavoro e privati.

III.3.1 **Contenuti della sentenza della Corte costituzionale sulla *Online Durchsuchung***

Dopo aver superato il primo ostacolo e aver accettato una decisione di merito, la Corte doveva: (a) decidere se il paragrafo 5.2 della legge sulla protezione della costituzione del Nord Reno-*Westfalia* era costituzionale; e (b) considerare più in generale la costituzionalità di questi metodi di investigazione.

La Corte statuì che il paragrafo 5.2 della legge sulla protezione della Costituzione nel Nord Reno-Westfalia, era non conforme alla Costituzione e pertanto nullo e privo di esecutività.

In particolare, la Corte ha preso in esame l'incostituzionalità di tale normativa sotto tre distinti profili: la riservatezza delle comunicazioni, l'inviolabilità del domicilio e il diritto all'autodeterminazione informativa.
Per quanto riguarda la riservatezza delle comunicazioni, art.10.1 GG, la Corte Costituzionale ha affermato che la protezione di questo diritto fondamentale copre ogni tipo di telecomunicazione a prescindere dal mezzo di trasmissione utilizzata (via cavo o radiotrasmissione, trasmissione analogica o digitale) e da tipo dei dati trasmessi (discorsi, immagini, suoni ecc.)[212].

Tuttavia, la Corte ha anche sottolineato che tale protezione

212 G.VACIAGO, *Digital evidence. I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato,* Giappichelli editore- Torino, 2012, pag.128.

non si applica, nel caso in cui i dati delle telecomunicazioni siano memorizzati all'interno di un computer dopo il termine della trasmissione.

Questo significa che il recupero di dati a distanza da un *hard disk*, non trova tutela nel diritto fondamentale alla riservatezza delle comunicazioni.

Per quanto riguarda il secondo diritto fondamentale analizzato, la Corte ha osservato che l'inviolabilità del domicilio, garantita dall'art. 13 GG, fornisce protezione solamente contro l'intrusione fisica in locali privati, effettuata allo scopo di manomettere i sistemi informatici ivi ubicati.

Il Governo federale ha sostenuto che la ricerca *online* sul *computer,* poteva essere comparata alla ricerca in abitazione, per cui l'art. 13 GG poteva essere usato come *standard* di riferimento.

Malgrado ciò, anche in questo caso, la Corte ha dichiarato che l'articolo 13 GG non era sufficiente a proteggere i diritti dei titolari contro un'intrusione nei sistemi tecnologici, finalizzata ad accedere ai dati e a monitorare le comunicazioni, anche se il sistema è situato in una casa.

Un problema specifico derivante dalle ricerche RFS è che le intrusioni e il monitoraggio possono essere eseguiti a prescindere dal luogo dove è situato il sistema tecnologico di informazione.

Quindi, una protezione dipendente dal luogo è inutile, se il

sistema si trova al di fuori dello spazio privato o in movimento tra aree protette. In particolare, i piccoli dispositivi tecnologici come portatili, PDA e telefoni cellulari sono progettati per essere trasportati.

Infine in merito al diritto relativo all'autodeterminazione informativa la Corte ha sostenuto che, benché esso tuteli gli utenti dalla raccolta dei dati e dalla loro successiva immissione in rete, l'attività di monitoraggio *online* va oltre la semplice raccolta di dati personali ai fini di profilazione. Difatti, l'accesso non autorizzato a qualsiasi sistema informatico, è atto di per sé idoneo a fornire dati altamente sensibili riferiti al proprietario.

Per tale ragione la Corte ha sostenuto che anche la tutela predisposta da tale diritto fondamentale era insufficiente.

In virtù di quanto detto, ci si sarebbe aspettati che la Corte ampliasse la disciplina sui diritti fondamentali e i principi costituzionali esplicitamente enumerati, invece, proprio la carenza della normativa costituzionale ha indotto la Corte medesima alla creazione *ex novo* di un diritto fondamentale denominato "riservatezza ed integrità dei sistemi tecnologici d'informazione".

Questo nuovo diritto non esplicitamente menzionato nella Costituzione, si desume dalla lettura in combinato disposto degli articoli 2.1(diritto allo sviluppo della personalità di ogni cittadino) e 1.1 GG.

L'articolo 1 GG (*Grundgesetz*), dispone che "la dignità

umana è inviolabile e tutti gli organi dello Stato hanno l'obiettivo finale di proteggerla", stabilisce, dunque, un generale principio fondamentale nel sistema legale tedesco ed è stato progettato esplicitamente come soluzione, per eliminare le lacune se le soluzioni legislative non rispettano il cambiamento sociale.

Dalla lettura del combinato disposto, si deve dedurre che il nuovo diritto costituzionale alla segretezza ed integrità dei sistemi tecnologici di informazione, ha la funzione di proteggere la vita personale e privata dei titolari dei diritti dall'accesso statale a dispositivi tecnologici di informazione, in particolare dall'accesso da parte dello Stato ai sistemi tecnologici di informazione nel loro complesso, non solo dunque per eventi di comunicazione individuale o memorizzazione dei dati.

Ad ogni modo, il diritto alla segretezza ed integrità dei sistemi tecnologici di informazione non è assoluto. Può essere limitato sia per motivi di prevenzione che per perseguire crimini.

Bisogna precisare, però, che qualsiasi misura limiti questo diritto fondamentale deve essere proporzionata alla violazione, soprattutto se la misura è eseguita senza la conoscenza del sospettato.

Quindi, la Corte ha rilevato che una misura che limiti questo diritto sia proporzionata, solo ove esistano prove sufficienti che significativi valori fondamentali di rango superiore

debbano essere protetti.

Valori fondamentali, di rango superiore, sono la vita e l'integrità degli altri cittadini, i fondamenti dello Stato e i valori essenziali di umanità.

Per di più, ognuna di queste misure deve essere esaminata e confermata da un giudice, con una decisione caso per caso, per garantire un controllo oggettivo ed indipendente prima dell'esecuzione e questo, deve trovare fondamento in una base giuridica costituzionale.

Conclusioni

L'analisi che si è svolta nel presente lavoro di tesi è volta ad indagare diversi nodi critici della materia della *digital evidence*.

Si è innanzitutto evidenziata la "rivoluzione tecnologica" determinatasi con la c.d. *Information and Comunications technology* regolamentata dalla Convenzione di Budapest del 2001, ratificata in Italia nel 2008.

Come conseguenza di tale evoluzione, la "*digital evidence"* ha assunto un ruolo fondamentale nell'ambito delle indagini preliminari.

A tal proposito, nella prima parte della trattazione si è scelto di soffermarsi su due fondamentali caratteristiche che connotano la *digital evidence,* ovverosia l'immaterialità e la fragilità, elementi che hanno fatto emergere la necessità

legislativa di adottare misure tecniche adeguate.

Nella ricerca di risposte a tali esigenze, è stato necessario volgere lo sguardo a tematiche e istituti propri del diritto di *common law* quali la disciplina della *computer forensics* e la pratica delle *best practices*, analisi che ha evidenziato numerosi profili critici dati dall'evidente difformità di tali strumenti rispetto al nostro sistema.

Tra i profili più problematici, si è evidenziata la fondamentale differenza inerente alla "gestione" della prova, soprattutto con riferimento al ruolo del giudice.

In conclusione a questi primi rilievi, è stato riconosciuto che il principio del contraddittorio sia oggi l'unico strumento capace di sondare l'effettiva validità delle ipotesi ricostruttive prospettate dalle parti, al fine di fornire al giudice medesimo gli elementi necessari per scegliere fra le varie teorie esposte.

Si è successivamente posto l'accento sul problema del *vulnus* della posizione difensiva dell'imputato al cospetto di una prova digitale "preformata" rispetto al dibattimento, il cui elemento chiave risiede nella facile modificabilità del contenuto.

Prendendo le mosse da questa questione, meritevoli d'interesse sono apparsi i profili legati alla natura ripetibile o irripetibile delle operazioni d'indagine informatica, così come quelli sulla natura sanzionatoria dell'inadempimento delle procedure operative impiegate dagli organi inquirenti.

Successivamente, si è evidenziata la necessità di tenere distinto il problema relativo alla delicatezza dei dati digitali

da quello relativo alle attività volte al loro reperimento.

Se è vero che le cautele utilizzate per preservare l'integrità della *digital evidence* sono in generale ben conosciute dal processualista, essendo già in parte applicate ad altri campi (come quello dei materiali genetici), la già sottolineata natura ontologicamente fragile del dato digitale chiama in causa un bagaglio più vasto ed incisivo di procedure atte a garantire l'attendibilità all'accertamento penale, che deve interagire con le norme codicistiche.

Ulteriore fondamentale coordinata della presente trattazione risiede nella constatazione di come la ricerca della prova digitale incida profondamente sui valori sanciti dalla Costituzione.

Nel capitolo centrale, dedicato ai mezzi di ricerca della *digital evidence*, è possibile denotare come la legge attuativa della Convenzione di Budapest abbia tentato di sistematizzare questo segmento investigativo.

E' stato evidenziato che, sebbene la novella non si sia occupata di plasmare gli istituti in maniera da risolvere la questione relativa al rispetto dei canoni di rilevanza e pertinenza nell'acquisizione della prova digitale, abbia d'altro canto mostrato grande attenzione al tema della genuinità della medesima.

Ci si è successivamente soffermati sulla questione relativa all'inutilizzabilità probatoria, come questione paradigmatica delle criticità della materia.

L'unica risposta plausibile dell'ordinamento ad una prova

formata senza il necessario rispetto dell'integrità della stessa, infatti, è una declaratoria di inutilizzabilità ai sensi dell'art. 191 c.p.p. e dei princìpi in materia di salvaguardia dell'integrità della prova digitale introdotti dalla l.48/2008.

Di certo, appare comprensibile come gli operatori sentano crescere il carico di lavoro nel settore delle indagini informatiche e con esso il rischio di veder frustrati gli esiti di investigazioni spesso complesse e articolate.

A conclusione di questa parte del lavoro, si è ritenuto di aderire all'orientamento di chi ritiene che il giusto percorso non possa essere quello di un abbassamento delle garanzie, per venire incontro ad una prassi che fatica a tenere il passo delle migliori pratiche scientifiche.

Si è rimarcato che il corretto itinerario da imboccare è piuttosto quello di una massiccia opera di formazione che conduca gli inquirenti a fare propri gli *standard* di acquisizione, nella consapevolezza che dietro ai metodi di acquisizione degli elementi digitali e alle tecniche di mantenimento della catena di custodia, si celano principi portanti del sistema e garanzie inviolabili dell'accusato.

Sempre il tema delle garanzie apre il varco all'ultimo argomento affrontato nel terzo capitolo del presente lavoro, dedicato alla *data retention.*

In tale ambito ci si è soffermati sulla recentissima decisione della Corte di Giustizia che l'ha dichiarata invalida.

Il sistema della *data retention*, ha statuito la Corte, si concreta in una violazione della Carta dei diritti fondamentali

dell'Unione Europea, ponendosi in contrasto con principi quali la libertà di espressione, la riservatezza della vita privata e la protezione dei dati della persona.

Procedendo nell'analisi dell'aspetto inerente al rispetto dei principi appena menzionati, si è ovviamente fatto riferimento alla nota decisione sulla *Online Durchsuchung.*

Si è evidenziato come, nella sentenza da ultimo menzionata, la Corte federale tedesca ha mostrato il suo orientamento, volto a contrastare un abuso del potere d'indagine a discapito di diritti inviolabili della persona.

Al termine della disamina, emerge in tutta la sua evidenza una conclusione, ovvero che il tema della *digital evidence* e delle attività d'indagine ad essa correlate lascia spazio maggiore ad interrogativi piuttosto che a soluzioni.

Un epilogo del genere, come è stato efficacemente sostenuto, non deve destare stupore: il penalista è ben conscio del fatto che nella scienza di cui si occupa "gli approdi sicuri non abbondano e che l'appalesarsi di un ormeggio provvisorio è spesso un risultato già apprezzabile" [213]

Si ritiene pertanto di aderire al monito di chi pone l'attenzione sui rischi della cosiddetta "tempesta digitale", che potrebbe facilmente condurre ad una deriva "tecnicista", atta a tramutarsi in un pericoloso *vulnus* alle garanzie intangibili.

L'unico criterio possibile per realizzare il miglior contemperamento dei diritti è quello di applicare i principi

213 L.LUPARIA, *Le scienze penalistiche nella "tempesta" digitale. Quali approdi?,* in *Arch. pen.,* 2013, p.882.

tradizionali del nostro ordinamento secondo metodologie differenti, che abbiano sempre presente la "bussola" dei valori fondanti il nostro modello di diritto e processo penale.

BIBLIOGRAFIA

ATERNO S., "Acquisizione e analisi della prova informatica", in Diritto Penale e Processo, 2008

ATERNO S., Nozioni ed elementi tecnici di principio, in Computer forensics e indagini digitali. Manuale tecnico giuridico e casi pratici, Experta, 2011.

ATERNO S., Acquisizione dati traffico ed intercettazioni telematiche in Computer forensics e Indagini digitali. Manuale tecnico-giuridico e casi pratici, Experta, 2011.

ATERNO S., Aspetti giuridici comuni delle indagini informatiche, in Computer forensics e indagini digitali. Manuale tecnico giuridico e casi pratici, Experta, 2011.

ATERNO S., La fase di acquisizione degli elementi di prova digitale: attività irripetibile o ripetibile?", (a cura di)

S.Aterno, F.Cajani, G.Costabile, M.Mattiucci, G.Mazzarco, in Computer forensics e Indagini digitali, Experta 2011

ATERNO S., "Modifiche al titolo III del terzo libro del codice di procedura penale", in Cybercrime, responsabilità degli enti, prova digitale, a cura di G. Corasaniti, G. Corrias Lucente, CEDAM, 2008

ATERNO S., Richiesta di consegna e sequestro dei dati digitali" in Computer Forensics e Indagini digitali, di S.Aterno, F.Cajani, G.Costabile, M.Mattiucci, G.Mazzarco, vol.1, Experta, 2011.

ATERNO S., CAJANI F., La disciplina in tema di conservazione dei dati, in Computer forensics e indagini digitali, Experta, 2011.

ATERNO S., CISTERNA A., Il legislatore interviene ancora sulla data retention, ma non è finita", in Dir. pen. e proc., 2009

BARTONE N., Mandato di arresto europeo e tipicità nazionale del reato, in Mandato di arresto europeo e procedure di consegna (a cura di Kalb), Milano, 2005.

BASSOLI E., Acquisizione dei tabulati Vs. Privacy: la data

retention al vaglio della Consulta, in Riv. Dir. dell'Internet, 2007

BENEDIZIONE L., PARIS E, Bilanciamento e dialogo fra le Corti nell'Unione europea: la Corte di Giustizia dichiara invalida la Data Retention directiva, in www.diritticomparati.it

BONO G., Il Divieto di indagini ad explorandum include i mezzi informatici di ricerca della prova, in Cass. pen. 2013

BRAGHO' G., L'ispezione e la perquisizione di dati, informazioni e programmi informatici, in Sistema Penale e Criminalità Informatica, a cura di L.Lupària, Giuffrè, 2009

BRUSCO C., La valutazione della prova scientifica, in Diritto penale e processo 2008

CAJANI F., ATERNO S., Aspetti giuridici comuni delle indagini informatiche", in Computer forensics e indagini digitali. Manuale tecnico-giuridico e casi pratici. Experta, 2011.

CAJANI F., Alla ricerca del file (perduto), in Diritto dell'Internet, 2006

CAJANI F., Internet protocol. Questioni operative in tema di investigazioni penali e riservatezza, in Diritto dell'Internet, 2008

CAJANI F., La rete internet e dintorni, parte I - Aspetti tecnici ed investigazioni di base, in Computer forensics e indagini digitali. Vol.II, Experta, 2011.

CAJANI F., Verso un nuovo concetto di cooperazione internazionale, in Computer forensics e Indagini digitali. Manuale tecnico giuridico e casi pratici, Experta, 2011

CALABRÒ V., COSTABILE G., FRATEPIETRO S., IANULARDO M., NICOSIA G., Alibi informatico. Aspetti tecnici e giuridici" in IISFA Memberbook, 2010

CAMON A., Le intercettazioni nel processo penale, Giuffrè, 1993.

CANZIO G., Prova scientifica, ragionamento probatorio e libero convincimento del giudice nel processo penale, in Diritto penale e processo, 2003, pag. 1194.

CATANIA E., Profili essenziali delle Intercettazioni Telematiche. Dalla tutela costituzionale della segretezza ed inviolabilità di qualsiasi forma di comunicazione alla

disciplina ex art. 266 c.p.p., in www.diritto.it.

CERQUA F., La Corte di Giustizia dichiara invalida la direttiva sulla Data retention: brevi osservazioni, in www.dirittopenaleeuropeo.it

CERQUA F., Il difficile equilibrio tra la protezione dei dati personali e le indagini informatiche, in Sistema Penale e criminalità informatica, (a cura di) L.LUPARIA, Giuffrè, 2009

COLOMBO E., La cooperazione internazionale nella prevenzione e lotta alla criminalità informatica: dalla Convenzione di Budapest alle disposizioni nazionali, in Cyberspazio e diritto, 2009

COLOMBO E., La sentenza del caso di Garlasco e la computer forensics: analisi di un complesso rapporto tra diritto ed informatica, in Ciberspazio e diritto, 2010

COLOMBO E., Data retention e Corte di Giustizia: riflessioni a prima lettura sulla declaratoria di invalidità della direttiva 2006/26/CE, in Cass. Pen., 2014

CORDI' L., Diritto alla privacy ed acquisizione di tabulati telefonici: repressione e garanzia nel crocevia tra Consulta e

legislatore, in Dir. pen. e proc., 2007

COSTABILE G., Scena criminis, documento informatico e formazione della prova penale, in Dir. dell'inf., 2005.

COSTABILE G., RASETTI D., Scena criminis, tracce informatiche e formazione della prova, in Cyberspazio e diritto, 2003

D'ANGELO L.A., La conservazione dei dati del traffico telefonico e telematico tra esigenze investigative e tutela della privacy, in Le nuove norme di contrasto al terrorismo, (a cura di) A.A.Dalia, Giuffrè, 2006

DANIELE M., Il diritto al preavviso della difesa nelle indagini informatiche, in Riv. Cassazione penale, 2012

DI MARTINO A., La frontiera e il diritto penale. Natura e contesto delle norme di diritto penale transnazionale, Torino, 2006.

DI PAOLO G., La circolazione dei dati personali e del casellario giudiziario" in Cassazione Penale, 2011

DI PAOLO G., La circolazione dei dati personali nello

spazio giudiziario europeo dopo Prum, in Cassazione Penale, 2010

DOMINIONI O., In tema di nuova prova scientifica, in Dir. pen. e proc. 2001

DOMINIONI O., La prova penale scientifica: gli strumenti scientifico-tecnici nuovi o controversi e di elevata specializzazione, Giuffrè, 2005.

FATTA C., La tutela della privacy alla prova dell'obbligo di data retention e delle misure antiterrorismo, in Dir. inf. e dell'informatica, 2008

FLOR R., Investigazioni ad alto contenuto tecnologico e tutela dei diritti fondamentali della persona nella recente giurisprudenza del Bundesverfassungsgerich: la decisione del 27 febbraio 2008 sulla Online Durchsuchung e la sua portata alla luce della sentenza 2 marzo 2010 data retention, in Ciberspazio e diritto, 2010

FLOR R., La Corte di Giustizia considera la direttiva europea 2006/24 sulla c.d.“data retention” contraria ai diritti fondamentali. Una lunga storia a lieto fine?”, in www.penalecontemporaneo.it.

GALANTINI N., L'inutilizzabilità della prova nel processo penale, Giuffrè, 1992.

LORUSSO S., Investigazioni scientifiche, verità processuale ed etica degli esperti", in Diritto penale e processo 2010

LUPARIA L., Computer crimes e procedimento penale in Trattato di procedura penale. Modelli differenziati di accertamento, a cura di G. Garuti, vol. VII, t.I, Utet, 2011.

LUPARIA L., I profili processuali, in Diritto Penale e Processo, 2008

LUPARIA L., Il caso "Vierika": un'interessante pronuncia in materia di virus informatici e prova penale digitale. I profili processuali, in Diritto dell'Internet, 2005

LUPARIA L., Processo penale e tecnologia informatica, in Riv. Dir. dell'Internet, 2008

LUPARIA L., Internet provider e giustizia penale, Giuffrè, 2012.

LUPARIA L., ZICCARDI G., Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali, Giuffrè, 2007.

MARAFIOTI L., “Digital evidence e processo penale”, in Cassazione Penale, 2011, pag. 4509

MORGANTE G., L.18/03/2008 n.48 – Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno (G.U 4.4.2008 n.80)”, in Legislazione Penale 2008

NAPPI A., Sull'abuso delle Intercettazioni, in Cassazione Penale. 2009

NEVOLI F., Intercettazioni informatiche e telematiche: ricorso ad impianti esterni ed obbligo motivazionale del pubblico ministero, in Arch.nuova proc.pen. 2010.

NOVARIO F., Le prove informatiche, in La prova penale, a cura di P.Ferrua, E.Marzaduri, G.Spangher, Giappichelli, 2013.

NOVARIO F., L'attività d'accertamento tecnico difensivo disposta su elementi informatici e la sua ripetibilità, in Riv. Ciberspazio e diritto, 2011

PARODI C., La disciplina delle intercettazioni telematiche, in Diritto penale e processo, 2003.

PICOTTI L., Sistematica dei reati informatici, tecniche di tutela e beni giuridici tutelati, in Il diritto penale dell'informatica nell'epoca di Internet, Padova, 2004

PISANI M. et alii, Manuale di procedura penale, 8a ed., Monduzzi, 2008.

RODOLFI A., Il regime normativo della data retention nell'ordinamento italiano. Stato attuale e problematiche concrete, in Cyberspazio e diritto, 2010

SALAZAR L., La lotta alla criminalità nell'Unione: passi in avanti verso uno spazio giudiziario comune prima e dopo la Costituzione per l'Europa ed il Programma dell'Aja, in Cassazione penale, 2004

SANSA F., ZAGARIA C., Caccia ai file nell'ufficio Sismi. I pm avviano la perizia sui pc, in La Repubblica, 14 luglio 2006, in www.repubblica.it.

SANTORIELLO C., La legge di ratifica della Convenzione di Budapest ed il nuovo diritto penale dell'informatica, in

Reati informatici. Nuova disciplina e tecniche processuali d'accertamento, (a cura di) G. Amato, V.S. Destito, C. Santoriello, Cedam, 2010

SANTORIELLO C., I reati informatici. Nuova disciplina e tecniche processuali d'accertamento, (a cura di) G.Amato, V.S.Destito,G.Dezzani, C.Santoriello, Cedam, 2010.

SENOR M. A., Legge 18 marzo 2008, n. 48 di ratifica ed esecuzione della Convenzione di Budapest sulla criminalità informatica: modifiche al codice di procedura penale ed al d.lgvo 196/03, in www.penale.it.

SOTTANI S., Rilievi e accertamenti sulla scena del crimine, in Arch. pen, 2011

SPANGHER G., Trattato di procedura penale, vol. 3°. Indagini preliminari e udienza preliminare, Utet giuridica, 2009

SPINELLA A., SOLLA G., L'identificazione personale nell'investigazione scientifica: DNA e impronte, in Cassazione penale, 2009

TAORMINA C., Diritto processuale penale, vol.I, Giappichelli, 1995.

TONINI P., Manuale di procedura penale, Giuffrè, 2012

TONINI P., Documento informatico e giusto processo, in Riv. Diritto penale e processo, 2009

TONINI P., Progresso tecnologico, prova scientifica e contraddittorio, in Diritto penale e processo 2003

UGOCCIONI L., Criminalità informatica in Legislazione penale, 1996.

VACIAGO G., Digital evidence. I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato, Giappichelli, 2012.

VACIAGO G., La Corte di Giustizia invalida la direttiva 2006/24/EU sulla data retention, in www.diritto24.ilsole24ore.com.

VACIAGO G., La disciplina normativa sulla Data Retention e il ruolo degli internet service provider, 2012.

VENTURINI S., Sequestro probatorio e fornitori di servizi

telematici, in Internet provider di L.Lùparia, Giuffrè, 2009.

VIGGIANO M., I dati personali nelle ricerche su internet, in Dir. inf. e dell' informatica, 2007

VITALE A., La nuova disciplina delle ispezioni e delle perquisizioni in ambiente informatico o telematico, in Riv. Dir. dell'Internet, 2008

ZICCARDI G., Privacy, sicurezza informatica, computer forensics e investigazioni digitali, Giuffrè, 2012.